Radio Frequency Identification and the San Francisco Public Library

Summary Report

Prepared by

San Francisco Public Library Technology and Privacy Advisory Committee

October 2005

Table of Contents

Acknowledgments

The San Francisco Public Library Technology and Privacy Advisory Committee (LTPAC) received significant support and assistance from a number of people to whom thanks are due. Deputy City Librarian Paul Underwood coordinated and attended all of our meetings, in addition to tracking down answers to numerous questions as they arose. Chief of the Main Library, Kathy Lawhun, also supplied key pieces of information on library operations and finances, whenever these issues came up.

The LTPAC was greatly served by presentations from two RFID specialists: Lee Tien, Senior Staff Attorney for the Electronic Frontier Foundation and U.C. Berkeley graduate student David Molnar. In addition to speaking at one of the Committee's meetings, Mr. Tien also graciously reviewed and added to the draft set of questions considered suitable for a Request for Information, which are included in this report.

Finally, several members of the general public attended some or all of our Committee meetings. A number of these individuals have spent considerable time working to bring attention to the issues raised by the prospect of implement RFID technology at the Library. All of them deserve credit for participating in the process of examining this technology.

Executive Summary

In early 2004, the San Francisco Public Library became interested in using Radio Frequency Identification (RFID) technology to achieve a multitude of goals, including reducing repetitive stress injuries, increasing the efficiency of circulation and collection management processes, and improving security. The proposed use of RFID raised significant concern among the public, specifically surrounding privacy, health and cost issues. As a result, the Library Commission created the San Francisco Public Library Technology and Privacy Advisory Committee (LTPAC), whose role would be to explore the technology and privacy issues associated with Library initiatives.

The first incarnation of the LTPAC was charged with investigating RFID, generating questions to include in a Request for Information to RFID vendors, and organizing one or more public educational workshops. The Committee began meeting monthly starting in April of 2005. In June of 2005 however, the funds that were earmarked for generating a Request For Information for RFID system vendors was transferred by the San Francisco Board of Supervisors to other Library programs. At that point, the LTPAC decided to conclude its work, capturing what had been learned to date in a summary report, which is this document.

During its tenure, the LTPAC explored the privacy, health, operational, security, and cost issues associated with using RFID systems in the library setting. Sources of information included library staff, issue experts, articles, vendors and others. The LTPAC considered the potential gain from such a system, as well as the potential risks of integrating RFID into the SFPL. The benefits the Library was hoping to achieve included reducing repetitive stress injuries, creating efficiencies in circulation tasks, redeploying staff to other patron-focused areas, improving collection management, and increasing security. The potential disadvantages that were raised included possible threats to privacy, the cost and uncertainty of the Return On Investment (ROI), the uncertainty of the quality of the performance, and potential effects on staff and patron health.

Almost all aspects of RFID in libraries require further investigation, whether those aspects are potential benefits or disadvantages. For instance, in the areas of performance, ROI, and operational efficiencies, a paucity of data exists from libraries with RFID systems. This will be partially addressed by an upcoming Bay Area Library Information System (BALIS) survey of RFID and California libraries. However, at the time of this report, conclusive data was not available.

In regards to health, a literature review of various health agencies found that currently available research and studies on radio frequency exposure to devices in the frequency range at which an RFID system for libraries operates do not suggest any health risks from radiofrequency (RF) exposures below guideline levels. However, agencies and organizations that have researched the possible health effects of RF on humans all agree that further research is needed to address uncertainties in current RF knowledge. In addition, health agencies advise that manufacturers of medical devices and security systems should provide sufficient information about current and new products to minimize the risks of emissions from security systems interfering with electrically powered active medical devices, such as pacemakers.

The possibility of breaching individual privacy comprised a large part of the LTPAC's discussion. An important point that arose was regardless of whether RFID is ever

implemented at the Library, privacy risks should be addressed throughout the library's operations and in particular when new systems (technical or other) are introduced. To assist the SFPL in this task, the LTPAC developed a set of recommendations to the Library, of which the most important was conducting a privacy audit to ensure that practices and policies are sufficient, up-to-date and responsive to the organization's privacy commitments and legal obligations.

While the LTPAC did not conclude its work in an RFI or with public educational workshops, it did create a set of questions regarding RFID for inclusion in future RFIs, as well as a bibliography. It is hoped that these resources will provide a useful starting point should there be an interest in exploring RFID in the future.

Committee History and Description

Background on RFID at the SFPL

The San Francisco Public Library began discussing the use of Radio Frequency Identification technology in 2004, with the inclusion of $300,000 for the first year of a six year rollout plan for an RFID system in the 2004/2005 budget. Some of the primary interests driving this interest included, but were not limited to:

- Reducing repetitive stress injuries (RSIs);
- Increasing the efficiency of check-in/check-out processes;
- Reallocating staff from circulation related activities to other patron services;
- Improving collection management; and
- Strengthening security.

In addition, plans to renovate 19 branches and enter into new construction at 5 sites were underway, presenting a unique opportunity to switch to a new system requiring new and different equipment. The Friends of the San Francisco Library had committed to raising $16 million to provide new furniture, fixtures and equipment for these 24 construction projects. These funds could, in part, support the purchase of more of the existing security equipment based upon electromagnetic technology or move into the new area of RFID technology with the result of saving the Library from using the Library's budgeted funds for the purchase of this equipment.

The Library Commission held an RFID forum on March 4, 2004 at which the following individuals made presentations:

Kathy Lawhun, Chief of the Main Library

Ms. Gail McPartland, Assistant Director, Peninsula Library System,

Ms Jackie Griffith, Director, Berkeley Public Library

Ms. Ann Brick ACLU, Northern California Chapter,

Mr. Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation,

Ms. Laura Quilter, Samuelson Law, Technology, & Public Policy Clinic, Boalt Hall School of Law,

Mr. David Molnar, Electrical Engineering/Computer Sciences Department, UC Berkeley

A question and answer session, moderated by Deputy City Librarian Paul Underwood followed, and public comments were taken. Items addressed included:

- Public health concerns with electro-magnetic technologies;
- Privacy concerns for library users;
- Process used to consider RFID;
- Potential benefits of RFID; and

- Repetitive stress injuries impacting library staff.

The Library Commission requested that more investigation be done before making a decision regarding the use of RFID. Specifically, they requested:

> An evaluation of the long-term cost and benefits, including potential improvements in the area of employee health;
>
> Development of written rules encompassing the best practices for its use;
>
> Consideration of what other libraries had done to implement RFID; and
>
> A review of questions about EMF (electro-magnetic frequency radiation) health related issues to address health concerns.

These issues and more were discussed at Library Commission meetings over the next several months, with additional input of information from staff, public commentary and further expert testimony. At the May 6th 2004 meeting, the Commission authorized funds for an RFID system and recommended that the Library work with vendors and critics such as the ACLU and EFF to test claims made by vendors.

At the June 17, 2004 Library Commission meeting, the Commission approved the Library's proposed Privacy Policy. Included in this policy are the following statements relating to RFID: "The only information stored on the RFID chip/tag will be limited to the item barcode or an encrypted number, as well as a security bit that indicates if the item is in or out of the library; RFID technology will not be used for library cards; and all local, state and/or federal legislation relating to RFID and library usage will be fully complied with at San Francisco Public Library."

At the August 19, 2004 Library Commission, Acting City Librarian Paul Underwood reported that the Board of Supervisors had approved the Library's 2004/2005 budget which set $300,000 on reserve for initial funding for an RFID system.

In the September and October 2004 Commission meetings, members of the public continued to express concern about RFID issues, such as the use of RFID in library cards, and expressed a desire for any process resulting in a Request for Proposal to include critics of RFID, to be very public, and to include public discussion.

In December 2004, the reserved RFID funds were liquidated from the 2004/2005 budget in response to a request by the Mayor's Budget Office to re-balance the Library's budget given the City's financial crisis. The $300,000 earmarked for RFID was only part of the Library's response to reach the total budget reduction of $513,000.

The 2005/2006 budget, however, included two-year's worth of funding for an RFID system in the Main Library, and the Excelsior, Glen Park, Mission Bay, Sunset, West Portal and Western Addition branch libraries, all currently in construction. The Commission approved the proposed budget at the February 17th Commission meeting with the proviso that the Library actively engage with critics of RFID to address concerns that had been raised from the public and from advocacy groups, particularly EFF and the ACLU. At a later date, the San Francisco Board of Supervisors' Library Citizens Advisory Committee also took a position cautioning against RFID technology in the library until health, privacy, workability and other concerns were satisfactorily addressed.

Formation of the San Francisco Public Library Technology and Privacy Advisory Committee

In order to meet the requirement to include RFID critics in the process of considering RFID, the Library created the San Francisco Public Library Technology and Privacy Advisory Committee (LTPAC) that as a body would be charged with exploring technology and privacy issues in relation to initiatives at the Library. RFID was designated as the first area on which to focus. Individuals representing differing viewpoints and expertise were contacted and requested to serve on this first incarnation of the LTPAC committee.

Within the context of that first area for investigation, RFID, the purpose of the committee was to develop questions that would be included in any RFI for an RFID system, to hold one or more public educational workshops on RFID, and to help structure an RFP should the decision to move forward be made. This committee was designated the San Francisco Public Library Technology and Privacy Advisory Committee (LTPAC), and was scheduled to meet monthly beginning in April 2005. Lee Tien of EFF and Ann Brick of the ACLU were invited to participate but declined.

Committee Members

Sybil Boutilier
American Library Association Intellectual Freedom Committee member; Manager of Contract Administration for the San Francisco Public Library

Karen Coyle
Digital Library Consultant

Steve Coulter
SF Public Library Commissioner; Vice President Public Affairs at Pacific Bell (ret.)

Deirdre K. Mulligan
Director, Samuelson Law, Technology & Public Policy Clinic; Acting Clinical Professor Boalt Hall School of Law, UC Berkeley

Melissa Riley
Labor Union Representative for Librarians

Chet Roaman
Council for Neighborhood Libraries Steering Committee member

Lisa Schiff
PhD, Library and Information Studies, UC Berkeley; Digital Ingest Programmer, California Digital Library

Nancy Terranova
Certified Safety Professional (CSP), Occupational Safety and Health Unit of the S.F. Department of Public Health

Mark Vogel
Founder and CEO of ENCIRQ Corporation (high performance data management solutions); Library Citizens Advisory Committee member; Friends of the San Francisco Public Library Board Member and former treasurer

Betty Williams
Labor Union Representative for Paraprofessionals

Summary of Committee Work

The LTPAC held its first meeting in April 2005 and was scheduled to meet monthly through July 2005. Some meetings were devoted to discussion among the committee members regarding the task of the committee, as well as general debate and discussion regarding RFID. Some meetings included presentations by experts, including Lee Tien of EFF, and David Molnar, who had previously addressed the Library Commission.

On June 30th, the San Francisco Board of Supervisors eliminated the funding for pursuing RFID at the SFPL, transferring those dollars to other Library programs. This decision was driven by concerns regarding privacy and health and letters and concerns from such groups as the EMR Policy Institute, San Francisco Neighborhood Antenna-Free Union, San Francisco Peace and Freedom Party, Council on Wireless Technology Impacts, ACLU Foundation of Northern California and three letters from private citizens.

The action by the Board of Supervisors meant that there were no longer any resources for crafting an RFI or holding a public educational workshop, which left the LTPAC without an urgent purpose or context for its work. Therefore, at the July 20th meeting, the committee agreed to capture its work to date in a summary report, extending the life of the committee until at least October 12th in order to complete that task.

Purpose of This Report

The goal of this report is to capture the results of the work of the LTPAC on RFID so that if RFID is reconsidered as an option, there will be a record of this preliminary investigation. While this report is intended to accurately summarize the work of the LTPAC, it is not intended to serve as an authoritative, exhaustive summary about any aspect of RFID systems and should not be taken as such. If the Library should contemplate use of RFID in the future, the information here is offered as background information.

RFID and Public Libraries

What is RFID and How Does It Work

Radio Frequency Identification (RFID) is emerging as the latest technological strategy in tracking goods and services, from pallets of CDs, to bridge tolls, to pets. RFID systems work by placing a chip with a small bit of data and an antenna on an item, enabling the data on that same chip to be accessed by a reading device.

RFID tags can be active or passive based, meaning that the chip either has or does not have an independent power source. Library applications currently use the passive tags, which are considerably less expensive than active tags. Passive tags are readable only when activated by a reading device, and have shorter read ranges than active tags.

RFID systems also vary in terms of radio frequency, depending upon the use. Low-frequency tags at less than 135 KHz are typically used for short-range uses, such as implants for pets. Library systems use the high-range 13.56 MHz frequency.[1] A third frequency, called Ultra-High Frequency, is at about 900 MHz and is for applications in which tags must be read at a longer distance.[2]

Several standards cover RFID systems, ISO 15693 for access control, the Standard Interchange Protocol for library automation systems, and ISO 18000, which sets standards for applications working with different frequencies. Although they adhere to these standards, the RFID systems designed for libraries use proprietary methods developed by the system vendors, and therefore are not interoperable among vendors.

Current Uses of RFID Other Than in Libraries

While the focus of the Library is of course on the use of RFID systems in libraries, it is important to be aware of that RFID is used in a variety of applications. Perhaps the most well known use is for electronic toll collection, such as the FasTrak system used in San Francisco Bay Area bridges. This system allows users to place a device in their cars that can be detected by a reader as the vehicle passes through a toll gate, triggering an automatic charge of the proper bridge toll against a user's credit card.

Pets have been implanted with RFID chips, so that if they get lost, they can more easily be reunited with owners. Chips are used to track pallets of goods, and some airlines such as Delta and British Airways are either investigation or have decided to use RFID to track luggage and prevent its loss. [3] [4] Vendors advertise RFID systems to help with tracking of

---

[1] David Molnar and David Wagner. "Privacy and security in library RFID: Issues, practices, and architectures." In Birgit Pfitzmann and Peng Liu, editors, *Conference on Computer and Communications Security -- CCS'04*, pages 210--219, Washington, DC, USA, October 2004. ACM, ACM Press. P. 3.

[2] "RFID Radio Frequency Identification: Applications and Implications for Consumers*." A Workshop Report from the Staff of the Federal Trade Commission.* March 2005. P. 7.

[3] Ron Coates, "Delta promises end to lost luggage with RFID" *Silicon.com.* July 1,2004. http://networks.silicon.com/lans/0,39024663,39121825,00.htm

[4] Jo Best. "Extending the Enterprise No more lost luggage: Airlines go for RFID*." Silicon.com.* June 6, 2005. http://www.silicon.com/research/specialreports/enterprise/0,3800003425,39130986,00.htm

pallets and containers of goods, fleet maintenance, car keys, tracking patients in hospitals and employee ID badges.[5]

The uses described above have for the most part not been controversial. Other proposed uses have. In particular, movement towards applying RFID to forms of identification, such as driver's licenses, employee identification cards and passports have all been met with concern.[6] In response to these potential uses, Senator Simitian and Assembly Member Evans of the California State Legislature co-authored the "Identity Information Protection Act of 2005", which as of late August 2005 was in suspension in the Senate as SB 682.[7] In addition to specifying measures required to be taken to protect identity information, this legislation explicitly prohibits the use of RFID technology in driver's license, K-12 school ID cards, health insurance or health benefit cards, and public library cards.

RFID and Libraries

RFID systems are being implemented for libraries as a replacement for the ubiquitous barcode system. Like barcodes, each item in the library will be tagged and the system will update the database as a tag is read. However, unlike barcodes, RFID tags do not have to be in the line of sight of a reader, which creates many potential opportunities and challenges.

Potential Benefits of RFID in the Library

The major benefits that are advanced fall into several areas:

Reduced time spent on circulation tasks: Because multiple identifiers can be read at one time, patrons and staff will spend less time for each check-out interaction. Libraries have stated that the savings in employee time could be used in other areas dealing with patron needs. Time and labor are reduced by:

- Decreasing the amount of time required by staff to handle a particular item on check-out and check-in, including difficult media such as videos and tapes;
- Increasing the use of self-checkout systems by increasing the number of such systems and the types of media they can accommodate; and
- Providing pre-sorting of returned materials.

The SFPL is especially interested in controlling the time required to support circulation tasks as upcoming renovations to the first floor of the Main library and 26 branches are anticipated to increase patron use of these sites. By 2009/2010, the Library estimates needing an additional forty half-time positions[8] to meet this increased demand.

---

[5] http://www.activewaveinc.com/

[6] Michael Kanellos . "E-passports to put new face on old documents " *News.com* August 18, 2004 http://news.com.com/E-passports+to+put+new+face+on+old+documents/2100-7337_3-5313650.html

[7] SB 682. http://www.leginfo.ca.gov/pub/bill/sen/sb_0651-0700/sb_682_bill_20050815_amended_asm.pdf

[8] San Francisco Public Library "RFID (Radio Frequency Identification) Tags & Libraries." February 25, 2005.

Increased Patron Privacy: Because more self-charge stations will be available, and because a greater number of media types can be handled by those stations, patrons will be able to check-out materials independently and with greater privacy.

Improved Shelf Collection Management: RFID provides inventory (collection) management capabilities. Staff can walk down a row of shelves with a reader which will instantly alert the shelver to any books that are misplaced or miss-shelved.

Decrease Tedious Aspects of Some Tasks: Time spent by staff on some circulation activities and on shelf-reading will be reduced, freeing staff for other tasks.

Improved Materials Management: An individual RFID tag serves both inventory and security purposes. Thus, staff must only attach one tag to a new item, as opposed to a barcode and a security strip.

Reduced Incidence of Theft: RFID promises to provide better security than the current magnetic strip system.

Expanded Security at Some Branches: The buildings of some branches are too old to accommodate the existing styles of security gates, therefore no security systems are in place. RFID security gates are smaller and could be installed in these buildings.

Reduced Rate of Repetitive Stress Injuries (RSIs): Because RFID tags do not have to be in the line of site of the reader, circulation staff will be required to do less manipulation of a given item. Such manipulation is considered a significant source of RSIs.

As part of the upcoming First Floor Main redesign project, the City's Bureau of Architecture contracted with Mike White of Mike White Consulting to study the most efficient way to process materials under the current 3M EMF security system. Mr. White is a board certified ergonomist and registered interior architect (CAE, AI) with over 25 years of ergonomic problem solving experience.

His study included time and motion evaluations of circulation activities including the check-in, check out and sorting tasks. Materials processed include books, DVDs, CDs and videos. Data was compiled after a series of meetings were held with affected staff, staff surveys were conducted and visual observations of the operations were made. The following is a summary of his findings, issued in a report dated April 10, 2003 (see Appendix A). This information was also presented to the Library Commission in April 2004 (see Appendix B).

Risk Factors – Excessive grasping and handling of materials requiring pinch grips, force and awkward postures to lift and turn material for scanning, de-sensitizing / re-sensitizing of non-magnetic material and opening VCR, DVD and CD cases.

Frequency of Tasks Performed

- **Return Desk:** Excessive grasping and handling of material to process returns totaling 10 events per minute / 575 per hour.
- **Check-Out Desk:** Awkward and excessive handling of material to process check out items totaling 12 events per minute / 768 per hour.
- **Sorting Room:** Excessive grasping and handling of material to sort and process returns totaling 16 events per minute / 940 per hour.

NOTE: Short cycle handling events such as these are considered "repetitive" when the number of events exceed 3 per minute. Therefore, under the current 3M EMF

security system processing returns and checking out and sorting materials are 3 to 5 times the rate considered "repetitive."

Principles of current EMF system that increases the number of repetitive hand activities are:

1. Each piece of material must be individually scanned and then separately de-sensitized / re-sensitized for non-magnetic material.
2. Fine hand motor skills are required to precisely line up the bar code on material with the scanning device for it to be read. In addition, materials must be frequently flipped and turned to access the bar code.
3. A forceful pinch grip is required when individually passing each piece of non-magnetic material over the sensitizer.
4. Magnetic materials must be processed separately from non-magnetic materials such as books.

Potential Disadvantages of RFID in the Library

Privacy:[9] Potential threats to privacy are the biggest concern being raised about RFID systems. Individuals have strong expectations of privacy in their choice of information content for reading, listening, and viewing. These norms are reflected in the policies of institutions, like libraries, that provide information goods, as well as statutory and constitutional protections. Individuals' expectations are informed by experience such as the ability to make cash purchases, browse information on the Internet or in a library, as well as law. Although library borrowing requires identification and registration, libraries have historically been staunch defenders of patron privacy, providing elaborate policy mechanisms to ensure records are kept secret from third parties when at all possible. Traditionally, libraries have championed First Amendment rights to free speech and freedom of inquiry, viewing themselves as determined defenders of due process in the face of threats to free and anonymous inquiry. In an Interpretation of the Library Bill of Rights, the American Library Association instructs that "[i]n a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others." To this end, "[r]egardless of the technology used, *everyone* who collects or accesses personally identifiable information in any format has a legal and ethical obligation to protect confidentiality." In addition to this broad policy statement, libraries' privacy policies typically implement Fair Information Practices—they hold patrons' information for the shortest time possible, keep minimal patron records, and restrict access to patron borrowing records, even where not required by law to do so.

Established public policy aligns with and reinforces these normative customs of relatively anonymous or confidential access to information. A patchwork of existing law protects the unique privacy interests in information goods from a number of would-be intrusions in a range of settings. While the privacy protections surrounding information goods are neither complete nor uniform, taken as a whole they reflect a core policy principle: that

[9] Much of this discussion is taken from the pre-publication long version of Good, Nathan et al. Radio Frequency Id and Privacy with Information Goods Paper given at the Workshop On Privacy In The Electronic Society. Washington, D.C., October 28, 2004. Washington, D.C. Association for Computing Machinery. It can be accessed here: http://www.law.berkeley.edu/clinics/samuelson/projects_papers/2004sp_rfid_WPES_draft.pdf

our democratic society guarantees the right to freely speak and listen without the potential chilling effect of personal identification with the subject at hand.

The Constitution protects individual rights of free and private inquiry against government intrusion in the First Amendment's prohibition of any law that abrogates freedom of speech.[10] and the Fourth Amendment's limits on government surveillance.[11] The Supreme Court has pronounced that the First Amendment protects the right to inquire freely as the logical corollary to freedom of speech: "The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read . . . and freedom of inquiry."[12] The Court has found that this right requires protecting the anonymity of speakers. One scholar points out that as new technology to monitor individuals' reading habits further develops, free speech increasingly depends on a right to read with relative anonymity.[13] Constitutional interests in open, surveillance-free use of information works limits the Government's power to discover the nature of its citizens' intellectual consumption. The Supreme Court provided a compelling example of this boundary in *United States v. Rumely*, holding that Congress could not compel a wholesaler of politically controversial books to disclose sales records at a congressional hearing.[14] The Constitution also limits the extent to which the Government can require citizens to disclose their choices in information access. In *Denver Area Educ. Telecommunications Consortium v. FCC*,[15] the Supreme Court struck down a statutory provision requiring subscribers of indecent cable television programming to first register in order to receive those programs. The Court found that the requirement abridged the broadcaster's speech rights and represented an unconstitutional restriction on individuals' right to view privately.[16] Further, the Court struck down a

---

[10] "Congress shall make no law …abridging the freedom of speech, or of the press." U.S. Const. amend. I.

[11] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV.

[12] Griswold v. Connecticut, 381 U.S. 479, 482. *See also* Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas."); (Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 64-65 n.6 (1963) ("The constitutional guarantee of freedom of the press embraces the circulation of books as well as their publication."); Smith v. California, 361 U.S. 147, 150 (1959) (stating that "the free publication and dissemination of books and other forms of the printed word furnish very familiar applications" of the First Amendment); Martin v. City of Struthers, 319 U.S. 141, 143 (1943) ("The right of freedom of speech and press has broad scope. . . . This freedom embraces the right to distribute literature . . . and necessarily protects the right to receive it."); Lovell v. City of Griffin, 303 U.S. 444, 452 (1938) (circulation of expressive material is constitutionally protected) (cited in Tattered Cover v. City of Thornton, 44 P.3d 1044, 1051 n.11 (Colo. 2002)).

[13] Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace"* . 28 Conn. L. Rev 981 (1996) P. 29.

[14] 345 U.S. 41 (1953). Though the Court declined to rule explicitly on First Amendment grounds because the committee in question was only empowered to investigate lobbying activities and bookselling could be considered outside its scope, Justice Frankfurter noted that the statute at issue carried "the seeds of constitutional controversy" and the Court was required to construe laws to preserve their constitutionality. *Id.* at 43-45. Explaining the privacy interest at stake, Justice Douglas wrote, "When the light of publicity may reach any student, any teacher, inquiry will be discouraged." *Id.* at 57 (Douglas, J. concurring).

[15] 518 U.S. 727 (1996).

[16] "[T]he "written notice" requirement will further restrict viewing by subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch

statute requiring individuals to identify themselves in order to receive controversial material, recognizing the burden such rules place on accessing information.[17] Protection of book sales records received keen public attention recently in the Kramer Books-Monica Lewinsky matter.[18] In 1998, Kramer sued to stop subpoenas from Independent Counsel Kenneth Starr for Monica Lewinksi's book purchase records. The store's owner stated that it is their company policy to "not turn over any information about [their] customers' purchases."[19] Kramer was successful in blocking Starr's subpoenas. Many organizations, including the Association of American Publishers, the American Library Association, the Publishers Marketing Association, and the Recording Industry Association of America, lauded the action and announced formal support for bookstore defense of consumer privacy as a matter of policy.[20]

Congress and state legislatures have created a patchwork of industry-specific statutes that shield records of individual inquiry from disclosure to public and private parties alike. These laws are generally based on Fair Information Practices and limit the collection, retention, and disclosure of data.

The heightened sensitivity to privacy with expressive materials is reflected in a number of federal laws. The statutory protections, while still patchwork and incomplete, are also typically stricter than for other goods. For example, at the federal level, the Cable Television Privacy Act of 1984 protects cable television subscribers from unfair data

---

the "patently offensive" channel. Id. at 754. *See also Lamont* v. *Postmaster General*, 381 U.S. 301, 307, (1965) (finding unconstitutional a requirement that recipients of Communist literature notify the Post Office that they wish to receive it); *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803

(2000) (striking down a statutory provision requiring scrambling or hours restrictions on the broadcast of adult programming and citing "the First Amendment interests of speakers and willing listeners—listeners for whom, if the speech is unpopular or indecent, the privacy of their homes may be the optimal place of receipt").

[17] *Lamont, DBA Basic Pamphlets v. Postmaster General*, 38 U.S. 301 (striking down a statute requiring the post office to ask intended recipients to confirm desire to receive Communist mail)

[18] *Supra* note 25.

[19] http://internet.ggu.edu/university_library/if/bookstore.html#challenge; The American Booksellers Association and the American Booksellers Foundation for Free Expression supported Kramer's move with an amicus brief. *Id.*

[20] Other supporters included the Freedom to Read Foundation, PEN American Center, the International Periodical Distributors Association, the Periodical Wholesalers of North America, the National Association of College Stores, the Periodical and Book Association of America, the Media Coalition, the American Civil Liberties Union, and the National Association of Recording Merchandisers. http://internet.ggu.edu/university_library/if/bookstore.html#challenge
In the Tattered Cover case, the government sought to identify the purchaser of a how-to book on making methylene through the records of a local bookstore. The bookstore won a challenge to the warrant on First Amendment grounds, the judge in the case noting that such a disclosure would implicate the expressive rights not just of the purchaser but of the entire book-buying public. Tattered Cover v. City of Thornton, 44 P.3d 1044 (Colo. 2002).The Colorado Supreme Court described the constitutional interest in information goods thus: "Bookstores are places where a citizen can explore ideas, receive information, and discover myriad perspectives on every topic imaginable. When a person buys a book at a bookstore, he engages in activity protected by the First Amendment because he is exercising his right to read and receive ideas and information."*Id.* at 1052. Colorado's constitutional protection of free speech is stricter than the federal floor, so it is not clear how the analysis might result in another jurisdiction

collection and use,[21] and the Video Privacy Protection Act protects the video rental records from release without a court order.[22] Similar laws protect library check-out and circulation information from release with without a court order in 48 states.[23] Moreover, the remaining two states have published opinions supporting the privacy of library borrowing records.[24] These laws mirror the express policy of the American Library Association. While legal protections are incomplete and not uniform between different types of information good providers, the practices of those who provide information goods—shaped by norms and law—are overall protective of private inquiry.[25]

Today providers of information goods, from wholesalers to retailers to renters and lenders, have control over their own records, and are often bound legally to demand due process of law before disclosing records reflecting the use or purchase of information goods. Libraries, book stores and others can examine subpoenas for authenticity and cause, and challenge them in court before disclosing private information. Librarians and

---

[21] 47 U.S.C. § 551 (2002).: (a) Cable providers must provide notice to subscribers regarding what personal data they collect, how they disclose and use it, and how subscribers may access their own data; (b) providers may not use the cable system to collect personal information other than as required to provide service; (c) providers may not disclose personal information without consent except as needed to provide service; even if served with a court order, providers must give subscribers notice and may not divulge individual programming choices; (d) providers must give subscribers access to their own personal data; and (e) providers must destroy personal data when it is no longer needed.

[22] 18 U.S.C. § 2710 (2002). Passed in 1998 in response to the disclosure of Supreme Court nominee Robert Bork's video rental records by a newspaper. Also grounded in FIP principles, the VPPA limits the parties to which video rental stores may disclose rental records to law enforcement with a warrant and civil litigants with a "compelling need," and requires stores to destroy rental records "as soon as practicable."

[23] "Eleven state constitutions guarantee a right of privacy or bar unreasonable intrusions into citizens' privacy. Forty-eight states protect the confidentiality of library users' records by law, and the attorneys general in the remaining two states have issued opinions recognizing the privacy of users' library records." See http://www.ala.org/Template.cfm?Section=stateifcinaction&Template=/ContentManagement/ContentDisplay.cfm&ContentID=14773; For instance, California state law provides: All registration and circulation records of any library which is in whole or in part supported by public funds shall re main confidential and shall not be disclosed to any person, local agency, or state agency except as follows: (a) By a person acting within the scope of his or her duties within the administration of the library. (b) By a person authorized, in writing, by the individual to whom the records pertain, to inspect the records. (c) By order of the appropriate superior court. As used in this section, the term "registration records" includes any information which a library requires a patron to provide in order to become eligible to borrow books and other materials, and the term "circulation records" includes any information which identifies the patrons borrowing particular books and other material. Cal. Gov. Code § 6267 (West 2004). *See also, e.g.*, Code of Ala. § 41-8-10 (Alabama); 75 ILCS 70/1 (Illinois); NY CLS CPLR § 4509 (2004) (New York).

[24] Id.

[25] *Infra*. Bookstores are not subject to the same legislative data protection requirements that libraries are in states that enforce library privacy laws. However, bookstores and other information good providers are "presumptively under the protection of the First Amendment" and hence subject also to the Fourth Amendment requirement that state actors seeking their records show reasonable cause and obtain a subpoena. Roaden v. Kentucky, 413 U.S. 496, 504 (1973). Nonetheless, it is important to note that much of the information good supply chain, including, publishers, warehousers, and distributors, remains largely unregulated, particularly concerning non-governmental invasions of privacy.

their legal counsel today often stand between their patrons and those who seek to know what their patrons read and view.[26]

Using RFID to tag information goods introduces a number of risks to personal privacy. Many of these risks are determined by the technical design of RFID readers and tags. RFID tags used for retail applications and tags used for libraries have significant distinctions. Retail tags are driven by technology developed for supply chain management. Tags are applied at manufacture and stay with the product during its life cycle. Retail tags may cost as little as 20 cents, with 5 cent tags envisioned within five years. Library tags, in contrast, are today applied individually by each library, remain with library holdings as they leave the library, and use a different set of technologies and tag labeling practices. Library RFID tag prices are in the 50-75 cent range.[27]

Libraries are typically interested in only storing unique identifiers on tags and not any bibliographic data. The unique identifier on the RFID tag identifies the individual book in the library's inventory. This identifier is stored in the library's database and connects the circulated book with its title. These identifiers are not visible in the public catalog. In addition, library vendors offer the capability of encrypting the data on the RFID tag, so no connection can be made between the identifier on the tag and the identifier in the database unless one is using the vendor's software.

This does not mean that tags cannot be read. Although encrypted, RFID passive tags will reveal their data to a reading device using compatible technology.

The privacy risks associated with library use of RFID tags storing only unique identifiers are three-fold.[28] Because current applications attach a static, unique identifier to each

---

[26] RFID technology also raises the unanswered question of what will constitute intentional interception of radio transmissions or unlawful access to information stored on RFID tags for purposes of the Wiretap Act as amended by ECPA. Violation of these laws requires a reasonable expectation of privacy on the part of the speaker, and such expectation may not be reasonable when an individual broadcasts information by radio frequency. 18 U.S.C.S. § 2510(2) (2000). Indeed, from 1986 to 1994 the law specifically exempted the radio portion of cordless phone conversations of phone conversations from protection because such transmissions were so easily intercepted. S. Rep. No. 541, 99th Cong., 2d Sess. 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566, cited in McKamey v. Roach, 55 F.3d 1236, 1239 (6th Cir. 1995). Though a subsequent amendment deleted the exception, courts have said that "broadcasting communications into the air by radio waves is more analogous to carrying on an oral communication in a loud voice or with a megaphone than it is to the privacy afforded by a wire." United States v. Hall, 488 F.2d 193, 196 (9th Cir. 1973), cited in United States v. Smith, 978 F.2d 171 (5th Cir. 1992) (noting that cordless phone conversations over radio frequencies are not subject to Fourth Amendment protection). To realize its purpose, ECPA may require further amendment or interpretation by courts that extends its protections to the radio transmissions of RFID.

[27] See Boss 2003. The high cost relative to retail tags is often explained by noting that libraries are a smaller market than retail, and that library tags must have lifetime durability measured in years rather than weeks or months as with retail tags. Library RFID applications must tag every single book, and many libraries have hundreds of thousands or even millions of books, so even small differences in the cost of a single tag can have a large impact on the total cost of implementation. Because of this cost, after a library invests in a particular tagging system it is very hard financially and in terms of time for libraries to switch implementations.

[28] See, Good, Nathan et al. Radio Frequency Id and Privacy with Information Goods Paper given at the Workshop On Privacy In The Electronic Society. Washington, D.C., October 28, 2004. Washington, D.C. Association for Computing Machinery. http://delivery.acm.org/10.1145/1030000/1029193/p41-

library item they facilitate tracking of two forms. First, RFID circulation items can be tracked as they flow from patron to patron and in and out of the library (hot-listing). A motivated individual can learn the unique identifier associated with a particular circulation item by using a reader compatible with the library's tags and then later either by using a compatible reader (skimming) or listening in on the communication between the library's reader and the item (eavesdropping) determine who is borrowing the tagged item. Second, because the RFID tags will respond to any compliant reader the tags can be used to track individuals who are carrying library circulation materials. Here the potential privacy loss is not related to the freedom of inquiry in that this would not disclose the nature or content of the tagged item, however it reduces privacy by providing a mechanism that facilitates the tracking of the individual's movement. Finally, while RFID in itself does not increase the exposure of a library's database, it may make that database a more appealing target, potentially increasing the number of attempts to illegally or inappropriately access it. For example, if a motivated individual wanted to discover surreptitiously what books an individual was reading he could capture the unique identifiers using a compatible reader and then attempt to access the database to obtain information about the authors and titles.

While the read range of library RFID tags using standard readers is currently modest (3 feet), antenna size can extend this range. In addition, readers are likely to become less expensive, more prevalent, and possibly capable of reading multiple frequencies. So while limiting information on the RFID tag to a unique identifier limits the privacy risks, it does not fully ameliorate the full range of privacy risks. It is essential that information about the library circulation item such as title, author and ISBN not be included on RFID tags. The underlying library data base must be amply protected to address the changing risk that RFID may introduce. However, the use of a static identifier of any sort poses challenges to privacy that have not been addressed by the current vendors.

Return on Investment (ROI): Installation of an RFID system is currently more costly than the equivalent system using barcodes, primarily because the tags themselves are many times more expensive than the barcode labels. After privacy issues, one of the biggest concerns with RFID is whether or not the investment will yield benefits worth the amount of investment.

In a memo dated May 2, 2004, the Library identified the costs for the materials required for an initial RFID implementation at the Excelsior branch and the Main Library. The total cost was estimated at $403,725, with the following item level prices:

- $0.55 per book, video, or audio tape
- $1.45 per CD/DVD
- $0.04 per item label
- $1,794 for installation of a station

---

good.pdf?key1=1029193&key2=8203898211&coll=ACM&dl=ACM&CFID=57028760&CFTOKEN=16066961

(longer version)
http://www.law.berkeley.edu/clinics/samuelson/projects_papers/2004sp_rfid_WPES_draft.pdf
Molnar, David, and Wagner, D.A. Privacy and security in library RFID: Issues, practices and architectures. June 8, 2004 http://www.cs.berkeley.edu/~dmolnar/library.pdf

- $3,000 for maintenance
- $9,000 for a self-charge station
- $14,000 for a staff circulation station
- $5,000 for a replication station
- $5,400 per pair of security gates

In addition, there may be costs not reflected here, including software and hardware, and repair due to vandalism when patrons try to remove the tags from the item. However, other factors, such as the reduction in staff time for check out and check in of materials, the elimination of the need for "tattle tape" inserts in items for security purposes, and the less tangible savings that could accompany the greater ability to perform inventories and identify missing and miss-shelved items, could bring the cost of the RFID system on a par with that of a system using barcodes. Some estimation of expected savings could be done based on the experience of other libraries, but the fact is that the data on ROI for library RFID systems is still scarce due to the early stage of implementation of this technology.

The costs of similar materials for the existing barcode system break down as follows[29]:

3M Security Strips

- ♣ $0.95 per CD/DVD
- ♣ $0.20 per video
- ♣ $0.125 per books

Barcodes

- ♣ $0.045 videos (triplicate at $0.15 each)
- ♣ $0.030 for books, CDs and DVDs (duplicate at $0.015 each)

Performance: Related to the questions regarding ROI, are questions regarding the performance of RFID systems. Relatively few library systems are using RFID systems, and those that have not been using them for very long. It is therefore difficult to determine if these libraries are satisfied with the systems that are in place.

Some of the specific concerns regarding performance are:

- The ability to defeat the security system by covering items in aluminum foil or other metallic materials that can block the radio waves;
- How well tags on CDs, DVDs and videos work in practice; and
- The precision of the inventory wands in identifying missing and misplaced items.

Health: The concerns regarding the impact on health from RFID technology is part of the general concern regarding the effects of electromagnetic frequencies on human beings. Health concerns are address in a subsequent section of this report.

[29] Figures supplied from a March 2004 analysis by SFPL staff member Vivian Pisano.

What Vendors are Offering Libraries

Vendors with barcode products are moving into the RFID product line as the "new technology" that they support. This is a time of transition, and the vendors are offering both their previous barcode solutions and RFID solutions (see Appendix B for a list of contacted vendors). Because it isn't clear if RFID will actually replace all uses of barcodes in libraries, and because many libraries need to make a gradual transition to RFID, many vendors have systems that can read both barcodes and RFID tags. All of the vendors are offering current barcode reading products that can be upgraded to RFID in the future as a way to help libraries that are not able or willing to make the RFID decision today but that wish to keep that option open. This, of course, also locks in the customer for future upgrades, so it is advantageous to the vendors.

The use of RFID tags among the vendors is very similar. Most vendors expect to carry only the barcode number on the RFID tag, and many of them offer encryption of that data. Note that use of encryption on the tags is not part of the RFID standard so encrypted tags can only be unencrypted with that vendor's software. While this provides greater security, it also means that it is not possible for a library to move to a different vendor without replacing all of the RFID tags in its collection.

What differs most in terms of vendor products is how RFID is used for exit gate security. There are two basic options: a "checked out" bit that can be changed as items are checked out. Any item leaving the library without this bit set to "checked out" will cause the gate alarms to go off. This requires the use of a read/write tag. The other option is that the gates will query the library database to determine if the item is checked out. This uses a read-only tag. Each solution has advantages and disadvantages.

Experiences of Libraries That Have Implemented RFID

The LTPAC did not have the time or resources to conduct a formal survey of libraries that have implemented RFID systems. Two small studies have been conducted fairly recently, but unfortunately neither study provides much detail.

In 2004, Infopeople and the Information Technology Section of the California Library Association conducted an online survey, inviting over 300 California libraries to participate[30]. Of those, 113 responded, only seven of which had actually implemented an RFID system. All libraries using an RFID system did so for security purposes, several for self-charge and circulation and one for inventory management. Some of these libraries reported problems with A-V materials and about half found that staff time spent on clerical work was reduced.

In 2004, Professor Jay Singhm, Navjit Brar, and Carmen Fong from California Polytechnic State University, conducted a one-month survey of libraries participating in the RFID and LITA-L listservs (see Appendix C for the complete results). Only 29 libraries responded, less than half of which had implemented RFID systems. Most of these respondents indicated that they were saving staff time and that circulation procedures had been quickened.

[30] A summary of the findings can be found online at: http://infopeople.org/resources/rfid_survey/

In the 2005/2006 timeframe a study will be conducted under funding provided by the California State Library that will look at methodology to determine return on investment for library RFID systems. This study will not itself make a determination of ROI but will provide metrics for future studies so that ROI information will be available in the future. It is expected, however, that reliable ROI information will need to be measured three to five years after the implementation of an RFID system, so definitive data is still some years in the future.

Health Effects of Library Radio Frequency (RF) Security Systems (RFID)

This section is a summary of current published studies addressing the health effects of exposure to radio frequencies. Reports cited address exposures to radio frequencies in the range of current library RFID systems. Review agencies include the World Health Organization (WHO), California Department of Health Services (DHS), National Council on Radiation Protection and Measurements (NCRP), a part of the UK Health Protection Agency, National Institute of Occupational Safety and Health (NIOSH), Federal Communication Commission (FCC), National Institute of Environmental Health Sciences (NIEHS), Institute of Electrical & Electronics Engineers, Inc. (IEEE) and International Commission on Non-Ionizing Radiation Protection (ICNIRP).

Background on Library RFID Systems

- RFID systems used in many libraries today transmit at a radio frequency of 13.56 MHz or 13.56 million cycles (waves) per second. These passive systems operate when activated checking media in or out or by passing through a security gate.
- Currently, RFID systems sold in the United States must receive a certificate from the Federal Communications Commission (FCC) indicating that they are in compliance with the thermal protection standard.

What is Radio Frequency Energy?

Radio waves and microwaves are forms of electromagnetic energy that are collectively described by the term "radiofrequency" or "RF". Radiation is defined as the propagation of energy through space in the form of waves or particles. Electromagnetic radiation can best be described as waves of electric and magnetic energy moving together (radiating) through space. These waves are generated by the movement of electrical charges such as in a conductive metal object or antenna. For example, the alternating movement of charge in an antenna used by a radio or television broadcast station or in a cellular base station antenna generates electromagnetic waves that radiate away from the "transmit" antenna and are then intercepted by a "receive" antenna. Examples include rooftop TV antennae, car radio antennae, and antennae integrated into a hand-held device such as a cellular telephone. The RF field can be described in terms of the electric and / or magnetic field strength at that location.

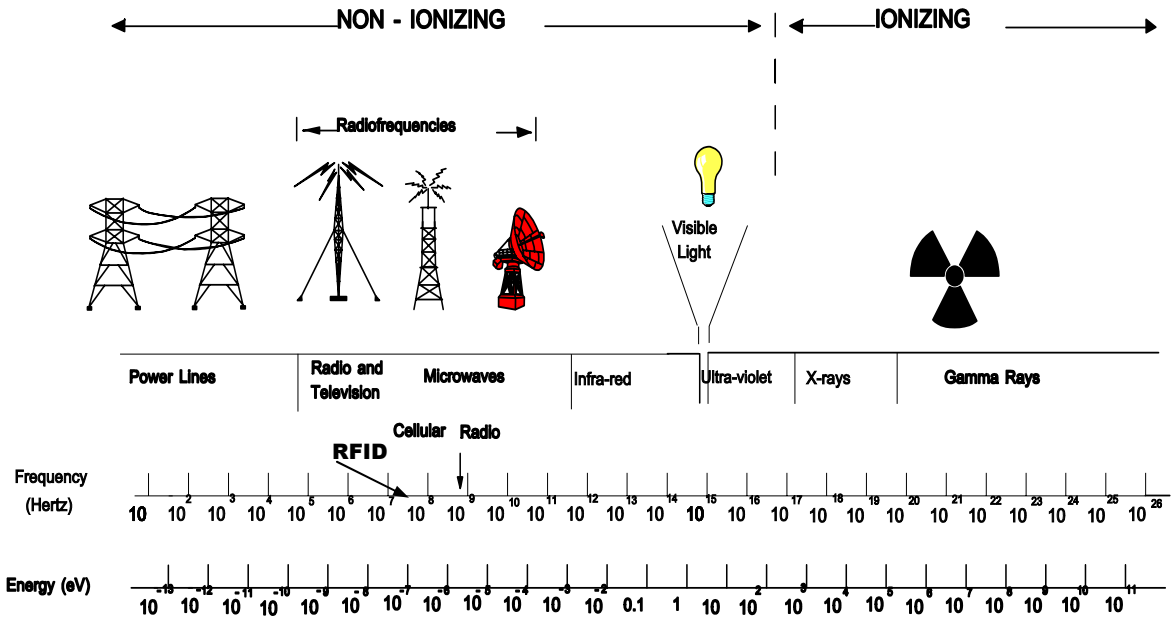
Electromagnetic energy can be characterized by a wavelength and a frequency. The wavelength is the distance covered by one complete electromagnetic wave cycle. The frequency is the number of electromagnetic waves passing a given point in one second. For example a typical radio wave transmitted by an FM radio station has a wavelength of about three meters and a frequency of about 100 million cycles (waves) per second or "100 MHz. "One "hertz" (Hz) equals one cycle per second. Therefore, in this case, about

100 million RF electromagnetic waves would be transmitted to a given point every second.[31]

The electromagnetic "spectrum" includes all of the various forms of electromagnetic energy, including ionizing radiation and non-ionizing radiation. Ionizing radiations are extremely high frequency electromagnetic waves, such as x-rays and gamma rays, which have enough photon energy to produce ionization (create positive and negative electrically charged atoms or parts of molecules) by breaking the atomic bonds that hold molecules in cells together. Non-ionizing radiations is a general term for that part of the electromagnetic spectrum which has photon energies too weak to break atomic bonds. They include ultraviolet (UV) radiation, visible light, infrared radiation, radiofrequency and microwave fields, extremely low frequency (ELF) fields, as well as static electric and magnetic fields.[32]

The RF part of the electromagnetic spectrum is generally defined as that part of the spectrum where electromagnetic waves have frequencies in the range of about 3 kilohertz (kHz) to 300 gigahertz (GHz). One kHz equals one thousand hertz, one GHz equals one billion hertz. When you tune your FM radio to 101.5, it means that your radio is receiving signals from a radio station emitting radio waves at a frequency of 101.5 million cycles (waves) per second, or 101.5 MHz..[33]

The Electric Magnetic Spectrum (see Appendix D for another representation)



[31] Federal Communications Commission Office of Engineering & Technology, OET Bulletin 56, August 1999.

[32] WHO Fact Sheet N182, "Electromagnetic Fields and Public Health," May 1998.

[33] Federal Communications Commission Office of Engineering & Technology, OET Bulletin 56, August 1999.

Health Effects of Exposure to Radio Frequency at Frequencies

Non-ionizing radiation covers a wide range of frequencies. These different frequency ranges have unique properties, and health effects reported in one range cannot be generalized to apply to all ranges. Different regions of the electromagnetic spectrum may affect biological systems differently. The known biological effects associated with these fields vary with the frequency and intensity of exposure. Intensity varies both with the amount of power emitted by the energy source and the distance of the individual from that source.[34] Strength of RF decreases quickly with an increase distance from the point source.[35]

Thermal Effects: Heating is the main biological effect of the electromagnetic fields of RF fields and is the principle employed to warm food with a microwave oven. Exposure to high levels of RF radiation can be harmful due to the rapid heating of tissue. However, the levels of radiofrequency fields that people are normally exposed to are much lower than those needed to produce significant heating.

- The heating effect of radio waves forms the underlying basis for current exposure guidelines.[36]
- The Institute of Electrical and Electronics Engineers, Inc., (IEEE), has stated that an extensive review of the literature on the health effects of exposures to RF electromagnetic fields revealed that the most sensitive measures of potentially harmful biological effects were based on the disruption of ongoing behavior associated with the increase of body temperature in the presence of electromagnetic fields.[37]
- The International Commission on Non-Ionizing Radiation Protection (ICNIRP) stated in their report on the possible health risks to the public from the use of security devices that exposures from security and similar devices are at levels many times below those that would induce a physiologically relevant heating.[38]

Non-Thermal Health Effects: Currently available research and studies on radio frequency exposure to devices in the frequency range of 10 MHz – 300 GHz do not suggest any health risks from RF exposures below guideline levels. The biological evidence does not suggest causal associations between exposures to RF fields and the risk of cancer.

Regulatory Standards for Radiofrequency Exposures

Exposure guidelines have been developed for both the occupational and non-occupational setting. For RF guidelines, the terms "controlled" and "uncontrolled" are sometimes used instead of occupational and non-occupational guidelines. Occupational or controlled exposure guidelines are usually higher than uncontrolled guidelines as they are intended

[34] NIOSH Facts – "Cellular Telephones: What do we know about the radiation they emit?"

[35] Department of Health Services – "Short Fact Sheet on EMF", 1999.

[36] Federal Communications Commission Office of Engineering & Technology, OET Bulletin 56, Fourth Edition, August 1999.

[37] IEE Std C95.1, 1999 Edition, "IEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz.

[38] International Commission on Non-Ionizing Radiation Protection, "Possible Health Risks to the General Public from the Use of Security and Similar Devices," 2002.

to apply to workers, who are adults. Uncontrolled guidelines are usually lower as they apply to the general population, which includes children and sensitive groups.

There are no mandatory federal or state (California) occupational RF exposure standards. Federal OSHA has issued a voluntary exposure limit for non-ionizing radiation in *CFR 29, Section 1910.97*. This is an advisory standard only and unenforceable by Federal OSHA. This standard strictly applies to the RF region of the electromagnetic spectrum and applies to continuous or intermittent radiation. It sets a "radiation protection guide" specifying the radiation level that should not be exceeded without careful consideration of the reasons for doing so. The guide states that for normal environmental conditions and for incident electromagnetic energy of frequencies from 10 MHz to 100 GHz, the radiation protection guide is 10 mW/cm^2 (milliwatt per square centimeter) as averaged over any possible 0.1 – hour period.

Federal, state, local governmental agencies, and other organizations have generally relied on RF exposure standards developed by expert non-governmental organizations such as the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers, Inc. (IEEE), the National Council on Radiation Protection and Measurements (NCRP), the Environmental Protection Agency (EPA) and the International Commission on Non-Ionizing Radiation Protection (ICNIRP). [39]

The FCC has adopted and used recognized safety guidelines for evaluating RF environmental exposure since 1985 based upon the recommendations of ANSI/IEEE, NCRP and the EPA. FCC guidelines incorporate limits for Maximum Permissible Exposure (MPE) in terms of electric and magnetic field strength and power density for transmitters operating at frequencies between 300 kHz and 100 GHz. MPE limits are specified for occupational controlled exposure and general population uncontrolled exposure. The FCC limits cover thermal exposure to products emitting RF radiation based upon data showing that the human body absorbs RF energy at some frequencies more efficiently than at others. Both the ANSI/IEEE and NCRP guidelines place the most restrictive limits on exposure in the frequency range of 30-300 MHz where the human body absorbs RF energy most efficiently when exposed in the far field of an RF transmitting source.[40]

Summary of Agency Reports of Health Effects from Radio Frequency at the Intermediate Frequency Range 10 MHz to 300 GHz

1. National Council on Radiation Protection and Measurements (NCRP)

The group examined recent studies related to assessment of health concerns related to exposure to RF fields including those arising from the use of cell phones. NCRP concluded:

- The weight of evidence now available does not suggest there are adverse health effects from exposures to RF fields below guideline levels.

[39] Federal Communications Commission Office of Engineering & Technology, OET Bulletin 56, Fourth Edition, August 1999.

[40] Federal Communications Commission Office of Engineering & Technology, OET Bulletin 65, Edition 97-01, August 1997.

- No biological evidence suggesting that RF field exposures cause mutation, initiate or promote tumor formation, or increase cancer risk.
- Current published research on RF exposures and health has limitations so continued research is needed.[41]

2. Federal Communication Commission (FCC)

The FCC issued a bulletin stating that:

- The possibility of "non-thermal" biological effects may exist. It is unknown at this time if these effects indicate a human health hazard. Further research is suggested to determine such effect and their relevance, if any to human health.
- In recent years, publications have appeared in scientific literature reporting observation of a wide range of low-level biological effects. In many of these cases further experimental research was unable to reproduce these effects.[42]

3. World Health Organization (WHO)

In 1996, WHO established the International EMF Project to address the public's concern regarding health effects of exposure to a diversity of electromagnetic fields (EMF) in private and industrial / commercial uses such as televisions, radio, computers, cell phones, microwave ovens, radars and medical equipment. The EMF Project looked at current knowledge and available resources from international and national agencies and scientific institutions to arrive at scientifically sound recommendations for exposure to EMFs including radiofrequencies in the range of 10MHz – 300 GHz (Intermediate Frequencies – IF). Their research included human and laboratory studies. They have concluded that RF fields in this range:

- Do not constitute a threat to human health and do not interfere with reproductive processes or pregnancy outcomes.
- No association between such exposures and eye abnormalities has been established.
- A large study on female radio and telegraph operators showed a slight increased risk of breast cancer. However, these workers were also exposed to many other factors that could explain this increased risk.
- Little laboratory research has been done on the effects of exposure in this frequency range.
- The scientific evidence is not convincing that adverse health effects occur from exposures to IF fields normally found in the living and working environment.

[41] National Council on Radiation Protection and Measurements (NRPB), "Health Effects from Radiofrequency Electromagnetic Fields: Report of an Independent Advisory Group on Non-ionizing Radiation",(AGNIR) 2004 and "Health Effects from Mobile Phones and Other Radiofrequency Sources, 2004.

[42] Federal Communications Commission Office of Engineering & Technology, OET Bulletin 56, Fouth Edition, August 1999.

- Additional research to address uncertainties in current knowledge is needed. [43]

4. International Commission on Non-Ionizing Radiation Protection (ICNIRP)

The ICNIRP issued a report in 2002 entitled, "Possible Health Risks to the General Public from the Use of Security and Similar Devices." In this report the ICNIRP reported the following findings.

- ♣ Heating, membrane stimulation and electroporation are responsible for most of the established hazards from acute exposure to electromagnetic fields. Generally relatively high field strengths or currents are required to pass directly into the body. Exposures from security and similar devices are at levels many times below those that would induce a physiologically relevant heating. ICNIRP's basic restrictions accommodate all known biophysical mechanisms in the EAS/RFID range. (EAS – Electronic Article Surveillance)
- ♣ In the intermediate frequency region, few animal and cellular studies have been carried out. The evidence to date concerning signal transduction, protein expression and cell proliferation is largely contradictory. Exposure studies have been done on adult males over a wide range of frequencies and exposure situations, but little data is available for adult females or children. Therefore, it is important to develop studies addressing the possible health effects due to differences in body size, anatomy and age.
- ♣ The identification of possible health risks from the use of security devices depends on the operating characteristics, specifically their operating frequencies, intensity of the produced electromagnetic field, details of their physical design and the pulse modalities used. There is a need to continue measuring the levels of exposure to people passing through and working near security systems.
- ♣ Although relatively infrequent, there have been incident reports suggesting that electrically powered active medical devices, such as pacemakers, worn by people walking through the security gates can have their medical function disrupted by emissions from the security systems. Therefore, it is recommended that manufacturers of medical devices and security systems provide sufficient information about current and new products to minimize the risks of emissions from security systems.[44]

Summary of Agency Conclusions

- ♣ Currently available research and studies on radio frequency exposure to devices in the frequency range of 10 MHz – 300 GHz do not suggest any health risks from RF exposures below guideline levels. The biological evidence does not suggest causal associations between exposures to RF fields and the risk of cancer.

[43] WHO, International EMF Project Information Sheet, "Electromagnetic Fields and Public Health – Intermediate Frequencies (IF), February 2005.

[44] International Commission on Non-Ionizing Radiation Protection, "Possible Health Risks to the General Public from the Use of Security and Similar Devices," 2002.

- Agencies and organizations that have researched the possible health effects of RF on humans all agree that further research is needed to address uncertainties in current RF knowledge.
- Manufacturers of medical devices and security systems should provide sufficient information about current and new products to minimize the risks of emissions from security systems interfering with electrically powered active medical devices, such as pacemakers.
- These conclusions were drawn after reviewing studies and reports issued by the World Health Organization (WHO), California Department of Health Services (DHS), National Council on Radiation Protection and Measurements (NCRP), a part of the UK Health Protection Agency, National Institute of Occupational Safety and Health (NIOSH), Federal Communication Commission (FCC), The National Institute of Environmental Health Sciences (NIEHS) and International Commission on Non-Ionizing Radiation Protection (ICNIRP).

Recommendations

- Continue to monitor current research on the health effects of exposure to radiofrequencies from RFID equipment (13.56 MHz) to verify whether new information indicates health risks. The agencies mentioned in this report are continuing to monitor research being done in this field.
- Ensure that any RFID equipment purchased:
- Meets the FCC requirements protecting users from any possible thermal effects.
- Includes all possible measures to minimize the risks of emissions from the system interfering with electrically powered active medical devices, such as pacemakers.
- Purchase of RFID equipment meeting the human exposure specifications of non-regulatory agencies such as the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers, Inc. (IEEE), the National Council on Radiation Protection and Measurements (NCRP), American Conference of Industrial Hygienists (ACGIH) and the ICNIRP.
- If RFID equipment is installed, conduct measurements of the radiofrequency emissions levels generated from systems to insure that the emissions are below those recommended under the OSHA non-ionizing standard (CFR 29, Section 1910.97) and by the non-regulatory agencies ANSI, IEEE, NCRP, ACGIH and ICNIRP.
- If RFID equipment is purchased insure that it is installed and maintained according to the manufacturers' specifications.

SFPL Staff Perspectives on RFID

No formal efforts have yet been taken to confidently determine the perspectives SFPL staff may have regarding the use of RFID. Clearly, part of any exploration of RFID would need to include efforts to educate staff regarding the variety of issues surrounding RFID and would also need to include efforts to solicit staff opinions and concerns.

Organizational Positions on RFID

The organizations below have been significant participants in discussions regarding RFID and public libraries.

American Library Association (ALA)
ALA has not taken a position either for or against RFID technology in libraries. Instead, on January 19, 2005, the ALA council adopted a resolution concerning RFID and privacy, which endorsed the Book Industry Study Group's policy statement on RFID, established privacy norms on accordance with existing privacy criteria for libraries, called for the continuing monitoring of RFID systems in regards to privacy concerns, and asserted the need for ALA to develop RFID implementation guidelines.

Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles

http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=85331

Book Industry Study Group Policy #002: RFID - Radio Frequency Identification Privacy Principles

http://www.bisg.org/docs/BISG_Policy_002.pdf

In addition to these positions, ALA's Intellectual Freedom Committee just recently developed a set of draft guidelines for RFID implementations at libraries. (See Appendix E.)

Electronic Frontier Foundation (EFF)
EFF has been actively involved in the debate over the use of RFID in the San Francisco Public Library. EFF is strongly opposed to the use of RFID technology in libraries on the grounds that the risks to privacy are too great and that the projections regarding cost savings are unreliable and do not justify the risk. EFF representatives have expressed these concerns to the Library Commission, the LTPAC, and the Board of Supervisors.

http://www.eff.org/Privacy/Surveillance/RFID/

ACLU
The ACLU has expressed serious concerns about the potential privacy and civil rights infringements posed by RFID technology. The organization has identified uses which it feels should be absolutely prohibited, such as forcing consumers to accept tags in merchandise. The ACLU has also specified acceptable uses of RFID, such as the tracking of pharmaceuticals up to the point of sale.

Local ACLU representatives have spoken out against the Library's proposed use of RFID technology at Library Commission meetings and through letters to the Board of Supervisors.

http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15559&c=207#3

San Francisco Community Organizations
The Library Citizens Advisory Committee

The Library Citizens Advisory Committee (LCAC) was established by the Board of Supervisors as a means for interested residents to discuss central issues of concern regarding the Library and to make recommendations to the Board of Supervisors. The use of RFID was one of the issues addressed by this committee. At its May 25, 2005 meeting several presenters from organizations such as the Electronic Frontier Foundation, the Breast Cancer Fund, and San Francisco Neighborhood Antenna-Free Union spoke

regarding concerns with RFID, including health and privacy issues. At that meeting, the LCAC made the following recommendation, expressing concern with the use of RFID:

"The LCAC recommends to the Board of Supervisors that no money should be allocated for RFID until the SFPL satisfies health, privacy, workability of RFID, and cost-benefit analysis concerns to the satisfaction of the LCAC."

http://sfpl.lib.ca.us/librarylocations/cac/minutes052505.htm

Library Users Association and the EMR Policy Institute

At the request of Peter Warfield of the Library Users Association, the EMR Policy Institute submitted several letters to the Board of Supervisors advising against the adoption of RFID at the SFPL due to the potential health risks associated with radio frequency technology.

San Francisco Neighborhood Antenna-Free Union (SNAFU)

SNAFU wrote to the Board of Supervisors expressing concern over the potential health risks from an RFID system, and also asserting that the money spent on such a system should be spent on books, staff and increased hours.

San Francisco Peace and Freedom Party

The San Francisco Peace and Freedom Party wrote to the Board of Supervisors objecting to the use of RFID at the SFPL because of potential risks to health and privacy, and because of the cost.

Council on Wireless Technology Impacts

The Council on Wireless Technology Impacts submitted a letter citing the potential health risks associated with RFID and the impact on residents who currently suffer from electrical hyper sensitivity.

Individual San Francisco Residents

Several individual San Francisco residents submitted letters to the Board of Supervisors protesting the use of RFID at the Library. Letters cited health concerns, the potential threat to privacy, and the cost.

Laws and Policies Relating to Library Privacy

Federal

Federal Family Educational Rights and Privacy Act of 1974. 20 USC 1232g.
Available on the Web at: http://www4.law.cornell.edu/uscode/20/1232g.html
"For the purposes of this section the term "directory information" relating to a student includes the following: the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student"
"Any educational agency or institution making public directory information shall give public notice of the categories of information which it has designated as such information with respect to each student attending the institution or agency and shall allow a

reasonable period of time after such notice has been given for a parent to inform the institution or agency that any or all of the information designated should not be released without the parent's prior consent."
"No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in education records other than directory information…. unless - (A) there is written consent from the student's parents…or… such information is furnished in compliance with judicial order, or pursuant to any lawfully issued subpoena, upon condition that parents and the students are notified of all such orders or subpoenas in advance of the compliance therewith"
"For the purposes of this section, whenever a student has attained eighteen years of age, or is attending an institution of postsecondary education, the permission or consent required of and the rights accorded to the parents of the student shall thereafter only be required of and accorded to the student

State

California Constitution Article 1 Declaration of Rights. Section 1. All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.
Ca. Gov. Code 6254(j) Library circulation records kept for the purpose of identifying the borrower of items available in libraries, and library and museum materials made or acquired and presented solely for reference or exhibition purposes. The exemption in this subdivision shall not apply to records of fines imposed on the borrowers.
Ca. Gov. Code 6267. All registration and circulation records of any library which is in whole or in part supported by public funds shall remain confidential and shall not be disclosed to any person, local agency, or state agency except as follows: (a) By a person acting within the scope of his or her duties within the administration of the library. (b) By a person authorized, in writing, by the individual to whom the records pertain, to inspect the records. (c) By order of the appropriate superior court. As used in this section, the term "registration records" includes any information which a library requires a patron to provide in order to become eligible to borrow books and other materials, and the term "circulation records" includes any information which identifies the patrons borrowing particular books and other material. This section shall not apply to statistical reports of registration and circulation nor to records of fines collected by the library.
Note: Records of fines are specifically exempt from Ca. Government Code Section 6254(j) and 6267
Ca. Information Practices Act. Ca. Civil Code Section 1798 et seq. "The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. The Legislature further makes the following findings: (a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies. (b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information. (c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits."

Available on the Web at: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798-1798.1

Ca. Gov. Code § 11015.5, "Electronically collected personal information" means any information that is maintained by an agency that identifies or describes an individual user, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, password, electronic mail address, and information that reveals any network location or identity, but excludes any information manually submitted to a state agency by a user, whether electronically or in written form, and information on or relating to individuals who are users, serving in a business capacity, including, but not limited to, business owners, officers, or principals of that business.

Local

San Francisco Environment Code. Chapter 1. Precautionary Principle.

[Excerpt]

" The following shall constitute the City and County of San Francisco's Precautionary Principle policy. All officers, boards, commission, and departments of the City and County shall implement the Precautionary Principle in conducting the City and County's affairs:

The Precautionary Principle requires a thorough exploration and a careful analysis of a wide range of alternatives. Based on the best available science, the Precautionary Principle requires the selection of the alternative that presents the least potential treat to human health and the City's natural systems. Public participation and an open and transparent decision making process are critical to finding and selecting alternatives.

Where threats of serious or irreversible damage to people or nature exist, lack of full scientific certainty about cause and effect shall not be viewed as sufficient reason for the City to postpone cost effective measures to prevent the degradation of the environment or protect the health of its citizens. Any gaps in scientific data uncovered by the examination of alternatives will provide a guidepost for future research, but will not prevent the City from taking protective action. As new scientific data become available, the City will review its decisions and make adjustments when warranted.

Where there are reasonable grounds for concern, the precautionary approach to decision-making is meant to help reduce harm by triggering a process to select the least potential threat. The key elements of the Precautionary Principle approach to decision-making include:

1. Anticipatory Action: There is a duty to take anticipatory action to prevent harm. Government, business, and community groups, as well as the general public, share this responsibility.
2. Right to Know: The community has a right to know complete and accurate information on potential human health and environmental impacts associated with the selection of products, services, operations or plans. The burden to supply this information lies with the proponent, not with the general public.
3. Alternatives Assessment: An obligation exists to examine a full range of alternatives and select the alternative with the least potential impact on human health and the environment including the alternative of doing nothing.
4. Full Cost Accounting: When evaluating potential alternatives, there is a duty to consider all the reasonably foreseeable costs, including raw materials, manufacturing, transportation, use, cleanup, eventual disposal, and health costs even if such costs are not

reflected in the initial price. Short- and long-term benefits and time thresholds should be considered when making decisions.

5. Participatory Decision Process: Decisions applying the Precautionary Principle must be transparent, participatory, and informed by the best available science and other relevant information." (Added by Ord. 171-03, File No. 030422, App. 7/3/2003)

Professional

ALA Code of Ethics 54.15 pt. 3. Librarians must protect each user's right to privacy with respect to information sought or received, and to materials consulted, borrowed or acquired;"

ALA Code of Ethics Section III. "We protect each library user's right to privacy and confidentiality with respect to information sought received and resources consulted borrowed, acquired or transmitted."

ALA Access to Electronic Information, Services and Networks: An Interpretation of the Library Bill of Rights. "Users have both the right of confidentiality and the right of privacy. The library should uphold these rights by policy, procedure, and practice, users should be advised however, that because security is technically difficult to achieve, electronic transactions and files could become public."

SAA Code of Ethics Section IX. Information about Researchers, "Archivists endeavor to inform users of parallel research by others using the same materials, and, if the individuals concerned agree, supply each name to the other party."

Sample Questions Suitable for an RFI

Operations and Performance:

1. Will you guarantee your system will interoperate with other vendors (e.g. self-check from vendor A, RFID tags from vendor B, staff workstations from vendor C)?

2. Explain how you ensure your system interoperates with other vendors.

3. Is a server required at each library location?

4. Please describe the barcode to RFID conversion process, including equipment needed and the ILS interface. Does your system provide for phased conversion and/or dual operations using both barcodes and RFID chips?

5. Describe the complete checkout and check-in cycle in a server-based environment.

6. Describe how your proposed system handles the following formats:

   - Print materials
   - Book with enclosed CD
   - Cassette tape
   - VHS videocassette
   - Compact Disc
   - CD-ROM
   - DVD-Video
   - DVD-ROM
   - Media Kits (Multi-media with one book or more in a case)
   - Any multi-piece items, all of which require making sure package and item match: e.g. book on CD with more than one CD; with more than 2 CDs)

   How successful is your handling of various non-print- and multi-media: for checkout, for checkin, and for security. What special coordinated or other chips do you use? Is repackaging of media required and if so for which media? Please describe. Do you provide those cases? If so, at what cost?

   Please describe any related problems and how you resolve them.

7. What happens when a server is unavailable? Do the staff workstations or self-check units continue to operate? What happens to security?

8. For each format, what is the check-in/checkout rate a library can expect with a near 100% accuracy (1, 3, or 10 items at a time)? What causes failures? Please describe the problems your system has with collision. What technological solutions do you use to avoid collision? Can you verify success rates in libraries?

9. Does your proposed system have, or integrate with any 3rd party, materials handling (conveying and sorting) systems?

10. Would a Staff station be capable of checking library materials in and out without need for Standard Interface Protocol (SIP) communication with the library's database? When operating in a non-SIP based mode, would the library's standard check out and check in screens remain open and fully operational?

11. How much information (in bits) can your RFID tag store?

12. How many tags can be read with circulation readers and units at once?

13. Describe how the RFID tag reader passes multiple tag reads to the circulation system in a way that it can accept it?

14. Specifically what data is stored on the tags for an appropriate system? What customization is allowed?

15. Give complete details on what data is actually on the tags in three different libraries where your system is installed?

16. Is there a verification process that checks that tags were programmed correctly?

17. How do proposed gates read RFID tags from other libraries?

18. Can the gates be programmed NOT to read RFID tags from other libraries? If yes, can the circulation readers still read the tags for circulation purposes?

19. How are tags deactivated, removed or replaced? (For discards, book sale items, errors, etc.) Can the tags indicate item was withdrawn? How?

20. What is the actual error rate of programmed tags in 3 different libraries where your system is installed? What kind of errors have been found?

21. Is there a specific location or locations for placement of tags for best reads?

22. Do your tags have a read/write design, operate at 13.56MHz or other frequency, and are they compliant with ISO18000-3 or some other standard?

23. Are your proposed tags capable of or feature an electronic article surveillance (EAS)security bit that is turned off automatically during check out and turned on automatically during check in? Do tags with an on bit issue an EAS security burst at 106KHz and require a "wake up call" for operation, operating therefore according to a "tag talk first" type of modulation?

24. Is an item's complete identification number (bar code number) stored in decimal format on the RFID tag? Is it visible? How would a visible number be affixed?

25. What is the memory capacity of your tags? 256 bits or greater or lesser?

26. What anti-collision capabilities do the tags possess allowing the reading of multiple tags simultaneously?

27. Do your RFID tags fit all standard types of library materials: books, magazines, CD/DVDs, audio books and video tape?

28. Are your tags tested for over 100,000 read/write cycles and are they guaranteed for the life of the items to which they are applied?

29. What tag anti-tampering strategies do you provide? For example, do you provide non-metallic based covering labels to protect the tag from intentional abuse? What other protection methods do you have available?

30. How do you recommend dual systems be handled—where both barcode and tags must be on every item until the library is fully installed?

31. Does the system turn security "on" or "off" on the tag?

32. Does the system track the circulation status for security?

33. Can the system record items that pass through the gates without having been checked out? If so how is the information recorded and reported?

34. Describe any devices that might errantly set off the gates (i.e., cell phones, pagers, PDAs, wireless devices, Items from other libraries, items from stores, etc.).

35. Please give all examples you are aware of regarding security problems at Library installations using your system. For example, how has a hostile patron been able to "beat the system"?

36. Do you have any statistics on false positives or negatives in libraries, and what causes them?

37. Do you have public circulating libraries which chose not to install security gates? Which chose not to tag media? Please explain.

38. How many items can be read in a stack without interference?

39. Describe how proposed system handles tag collisions. What are the results of tag collisions?

40. What is the speed of proposed anti-collision reads?

41. Describe how proposed system handles reader collisions. What are the results of reader collisions?

42. What are the data transfer rates for proposed equipment and tags?

43. What carrier frequency is used?

44. What is the read range of proposed tags? Please provide actual test data indicating greatest possible read range, using readers much more powerful than yours (specify).

45. What is the field range of proposed interrogators? Please provide actual test data indicating greatest possible field range

46. How close/far apart are reader/interrogator requirements?

47. Describe any known interference with other systems and devices such as computers, laptops, cell phones, wireless devices, items containing metal, etc. Is there any known interference with facilities and/or construction?

48. What is the practical read rate per second of your system?

49. What is the read range of the hand-held wireless inventory wand?

50. Explain any facility issues a library must consider in a wireless environment.

51. How far from gates or readers would you recommend staff seats or desks be placed?

52. What are the checkout and/or failure rates for a "mixed bag" of materials in different formats?

53. What is the rate of successful checkout versus failure for actual RFID installations as well as any laboratory testing you have conducted? What are the rates that libraries using your system have actually experienced?

54. Installation: please describe process and length of time per various kinds of items. Can this be done at the shelf? Or only at a stable location? How?

55. Please describe inventory process. How far from its correct placement must an item be before it is detected as miss-shelved.

56. Please describe any automatic sorting options.

Hardware:

1. Is a central server required to communicate with our ILS? What are the requirements of the central server if answer is yes?
2. What ISO standard are your tags? Are the tags proprietary?
3. Do you use read only or read/write tags? Explain your response.
4. Can off-the-shelf readers read your tags, for example using Lukas Greenwald's RF-DUMP software or other available software?
5. Provide physical dimensions and power requirements of all RFID components.
6. Describe the physical aspects of the hand-held wireless inventory device. Please include weight and dimensions.
7. Do any of the antennas used at the self-check or the circulation desk have RF bleed over, if so, how many inches?

8. What install/model options are available for security gates? We currently have 3M gates installed.
9. Will you cooperate in and facilitate a third party analysis of your system components?

Service and Support:

1. Describe all warranties available with any hardware or software that is installed as well as guarantees of the vendor work if any. What is the expected life of all equipment?
2. Do you have a trade-in program for non-RFID security equipment?
3. How will you handle software/hardware updates and forward developments in chip technology?
4. Please explain the enhancement and upgrade process for the proposed system.
5. How are you planning for forward compatibility?
6. What levels of staff and technical training and documentation are available?
7. Where is your nearest service and maintenance staff located?

Security and Privacy:

1. Does the RFID tag have a portion of memory that can be locked (for item number) and a portion that can be re-programmed?
2. What encryption methodologies are available for your RFID tags?
3. Does the RFID tag have or not have a pre-programmed number that would be rendered redundant by unique library item number?
4. Do your RFID tags contain a manufacturer burned-in static ID number that cannot be changed by the library, such as for use in a collision-avoidance protocol?
5. Do your tags have a completely silent mode? Can they be "reawakened" from that mode?
6. What information can still be read in the "silent mode" Is there a static identifier built into the chips, such as manufacturer or customer number?
7. Are there access controls, like passwords or keys, which prevent unauthorized readers from reading the tags? If so, do authorized readers first authenticate themselves to the tags, or do tags reveal their IDs first?
8. If passwords or keys protect the RFID tags from unauthorized reading, are the same passwords or keys used by all of your systems, so that one library's readers can read another library's tags? Or are passwords or keys different for each of your systems?

9. If the system uses passwords or keys, how does a reader know which password or key to use? Do readers contain all passwords or keys?

10. Describe the encryption algorithm used with your system in a wireless environment.

11. Who can write to the tags?

12. How can tags be locked so that unauthorized parties cannot write to them?

13. Can the Security Bit be locked by an unauthorized party so that the library cannot unlock it again?

14. Do your tags support the option of writing a random ID to the tag on every checkout, with the library database retaining a map of the random ID to the item's number?

15. How do you address privacy concerns? Please detail.

Safety and Health

1. Is the system compliant with ADA and other federal regulations?
2. Do you have any evidence of how the use of RFID at libraries affects the incidence of repetitive stress injuries? Please provide details.
3. Do you have data listing the radio frequency (RF) exposure levels emitted from a properly functioning system? If so, what are the exposure levels?
4. If no RF exposure levels are available, may we visit libraries using your system and take measurements of radio frequency levels?
5. Is the RF exposure level from your system below the OSHA voluntary exposure limit for non-ionizing radiation (CFR 29, Section 1910.97)?
6. Are RF exposure levels from your system within the recommended standards issued by ANSI, the IEEE, NCRP, EPA and ICNIRP?
7. How do you address health and safety concerns? Please detail.

Customer References

1. What are your 10 oldest and 10 newest RFID installations? (please include similar installations at other than libraries if you do not only serve the library market).
2. What implementation problems were encountered and how were they solved?
3. Provide us with contact information for each of your installations referenced above.
4. May we visit libraries using your system and test to see how far the tags can be read?

Recommendations to the Library

During the course of its discussions, the LTPAC identified a set of recommendations for the Library to consider. All except one, conducting a privacy audit, are specific to RFID. The need for a privacy audit stood out as an important task to undertake irrespective of the future of RFID at the Library, as no matter which technologies and systems are in place, privacy concerns always must be addressed.

RFID Specific

1. Obtain and carefully consider the findings of the California State Library funded survey of RFID implementations when they are issued.
2. Solicit staff opinions, ideas and concerns regarding the use of RFID at the Library.
3. Organize one or more educational forums about RFID for the general public and staff.
4. Rigorously research the ROI of RFID. This task will be aided by the results of the California State Library study.
5. Investigate the implications of San Francisco's Precautionary Principle in regards to implementing relatively new technologies such as RFID.
6. Complete an RFI to RFID vendors using information obtained from addressing the previous recommendations, the report of the LTPAC and other sources. Producing an RFI was discussed as a means of influencing RFID vendors to address issues of special concern to libraries, especially privacy.

Privacy Audit

The San Francisco Public Library has policies regarding the confidentiality of library records and general privacy of patrons who visit the library. These policies make clear the intentions of the library, but action on the part of the library is required to make these policies a reality. In particular, the library needs to perform an inventory of all places where data is gathered that could reveal the identity of a patron and their use of library materials. This inventory should be followed by a technical audit that would determine the security of the data involved.

In addition, the library should study its own data gathering practices to see if these adhere to the intentions of the library privacy policy. The questions are: Do we know what data is gathered and stored by all of our library systems (web sites, ILS, OPAC, licensed services)? How long is it stored? Do we remove data that is no longer needed?

The Committee encourages the SFPL to take the steps necessary to perform a valid privacy audit, and to use this audit to bring library practice into conformance with its privacy policy. An audit is a complex task, and therefore it may be best to tackle this in phases so that the impact on the library staff is minimized. Some possible division of the task into phases might be:

1. Survey all library departments for a list of records, temporary or permanent, that relate to patrons and patron activity. Note where the data is stored.

2. Using that list, identify high, medium, and low priority records. Beginning with the high priority records and moving through the entire list, answer the questions:

   a. Is any data being gathered that is not strictly necessary to perform the work of the library?
   b. Which staff must have access to this data to perform their duties? Are there other staff who have access to this data today, and can their access be limited in the future?
   c. How long is the data being stored? Are there records-keeping policies that pertain to the storage of this data? Is data purged when it is no longer needed?
   d. Is the data stored in a secure environment?

3. For computer systems, determine if a professional audit of the security and practices is feasible. This may require special funding so planning should take this into account. The results of steps 1 and 2 can be used to develop a plan and provide justification for a security audit.

4. The Committee encourages the SFPL to continue to implement existing privacy policies vigorously. This includes regularly ensuring that all staff, but especially those members dealing directly with the public, are adequately trained in the standard applications of such policies at SFPL, and that SFPL re-examine their practices regarding privacy when introducing new technologies, policies, and procedures. In addition, standard training and orientation procedures should be regularly reviewed to ensure that they include up-to-date information regarding privacy policies.

RFID Resources

Libraries and RFID

_____ *California Library RFID Study* Infopeople, August-September, 2004 http://www.infopeople.org/resources/rfid_survey/

_____ *Overview of library RFID products.* in: Libramation, 2004 http://www.libramation.com/prod_radio.html

_____ *Should Libraries Play Tag with RFIDs?* American Libraries, December, 2003. pp. 69-71

American Library Association *Code of Ethics of American Library Association.* http://www.ala.org/ala/oif/statementspols/codeofethis/codethics.htm

Artz, M *City library adopts controversial RFID Chips* Berkeley Daily Planet. October 10, 2003 http://www.berkeleydailyplanet.com/article.cfm?archiveDate=10-10-03&storyID=17547

Artz, Matthew *Library's New Technology Sparks Controvery* in: Berkeley Daily Planet, February 15, 2005 http://www.berkeleydaily.org/article.cfm?archiveDate=02-15-05&storyID=20728

Ayre, Laura B *Position paper: RFID and libraries. Working draft.* August 19, 2004 http://www.galecia.com/weblog/mt/archives/cat_rfidandwireless.php

Ayre, Laurie B *RFID and Libraries* August 19, 2004 http://www.galecia.com/weblog/mt/archives/cat_rfidandwireless.php

Boss, Richard W *RFID technology for libraries.* ALA Tech Notes. May 14, 2004 http://www.ala.org/PrinterTemplate.cfm?Section=technotes&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=68138

Carlson, S *Talking tags: new high-tech labels help libraries track books, but worry privacy advocates. The Chronicle of Higher Education.* August 6, 2004 http://chronicle.com/free/v50/i48/48a02901.htm

Chachra, Vinod *Experiences in implementing the VTLS RFID solution in a multi-vendor environment* Presentation at 69th IFLA General Conference and Council, 2003. http://www.ifla.org/IV/ifla69/papers/132e-Chachra.pdf

Flagg, G *Should libraries play tag with RFID?* in: American Libraries, 34(11), December, 2003. pp. 69-71. Chicago: American Libraries

Lindquist, M. G. *RFID in libraries - introduction to the issues. Presentation at 69th IFLA General Conference and Council, 2003.* August, 2003 http://www.ifla.org/IV/ifla69/papers/161e-Lindquist.pdf

Research Information. *Radio-tagged books: Why librarians should switch on their books.* May/June, 2004 http://www.researchinformation.info/rimayjun04radiotagged.html

Schneider, Karen *RFID and libraries: Both sides of the chip.* November 19, 2003 http://www.senate.ca.gov/ftp/SEN/COMMITTEE/STANDING/ENERGY/_home/11-20-03karen.pdf

Schneider, Karen G. *RFID and Libraries: Both Sides of the Cup* November 19, 2003

Warfield, Peter and Lee Tien *RFID: Many Problems, Little Public Discussion* In: Berkeley Daily Planet, April 8, 2005. http://www.berkeleydailyplanet.com/article.cfm?archiveDate=04-08-05&storyID=21128

RFID Technology

_____*ISO/IEC 18000 - RFID Air Interface Standards* Geneva, International Standards Organization

_____*RFID 101: The Future is Here* In RFID Gazette, June 28, 2005 http://www.rfidgazette.org/2004/06/rfid_101.html

AIM Global *Technologies: RFID* http:P//www.aimglobal.org/technologies/rfid/

EPC Global *Guidelines on EPC for Consumer Products.* http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html

Federal TradeCommission *RFID Radio Frequency Identification: Applications and Implications for Consumers* Washington, D.C., FTC, March, 2005.

Garfinkel, Simson *RFID: applications, security, and privacy* Upper Saddle River, NJ, Addison-Wesley, 2005

Mayfield, K *Radio ID Tags: Beyond Bar Codes. Wired News.* May 20, 2002 http://www.wired.com/news/technology/0,1282,52343,00.html

PeopleSoft *Improving Performance with Radio Frequency Idnetification (RFID)* PeopleSoft What Paper Series. Pleasanton, CA, April, 2004.

Shepard, Steven *RFID: Radio frequency identification* New York, McGraw-Hill, 2004

Sweeney, Patrick J. *RFID for Dummies* Hoboken, N.J. : Wiley, 2005

Want, Roy *RFID, a Key to Automating Everything* in: Scientific American, January, 2004. pp. 57-64

Ward, Diane Marie *RFID Systems.* Computers in Libraries, March, 2004 pp. 19 - 24.

Best Practices

Berkeley Public Library *Best practices for library RFID* Berkeley, 2004 http://berkeleypubliclibrary.org/BESTPRAC.pdf

Berkeley Public Library *Best Practices for RFID technology.* http://berkeleypubliclibrary.org/BESTPRAC.pdf

Cavoukian, Ann *Guidelines for Using RFID Tags in Ontario Public Libraries* Ontario, Information and Privacy Commissioner, June, 2004. 12 p.

Givens, Beth *RFID implementation in librarians: Some recommendations for "Best Practices."* Summary of presentation to the ALA Intellectual Freedom Committee of the American Library Association at the ALA Mid-Winter Conference, San Diego, California. January 10, 2003 http://www.privacyrights.org/ar/RFID-ALA.htim

Health Issues

California. Department of Health Services. California Electric and Magnetic Fields Program *Short Factsheet on EMF* Sacramento, Department of Health Services, 1999. 4p

Federal Communications Commission. Office of Engineering and Technology *Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields* OET Bulletin 56, 4th Edition. Washington, D.C., FCC, August, 1999. 36 p.

International Commission on Non-Ionizing Radiation Protection *Possible Health Risks to the General Public from the Use of Security and Similar Devices: Executive Summary* Oberschleisheim, ICNIRP, 2002. 18p. ISBN 3-934994-02-4

Pacific Gas and Electric Company *Understanding EMF: Electric and Magnetic Fields* PG&E, December, 2004
World Health Organization *Electromagetic Field Project* http://www.who.int/peh-emf/en/
World Health Organization *What Are Electromagnetic Fields?* Geneva, World Health Organization, n.d. http://www.who.int/peh- emf/about/WhatisEMF/en/index.html

Organizations

Amateur Radio RF Safety Calculator. http://n5xu.ae.utexas.edu/rfsafety/
California Electric and Magnetic Fields Program (Part of the California Department of Health, Environmental Health Investigations Branch.) http://www.dhs.ca.gov/ps/deodc/ehib/emf/
EMR Network. http://www.emrnetwork.org/
Federal Communications Commission, Office of Engineering and Technology. Radio Frequency Safety. http://www.fcc.gov/oet/rfsafety/
International Commission on Non-Ionizing Radiation Protection. http://www.icnirp.org/
Pacific Gas & Electric, Understanding Electric and Magnetic Fields website. http://www.pge.com/education_training/about_energy/emf/
Sage EMF Design, Environmental Consultants. http://www.sageassociates.net/radiofrequency.html
San Francisco Neighborhood Antenna-Free Union (SNAFU). http://www.antennafreeunion.org/
Sutro Tower Community Perspectives. http://www.sutro.org/
National Institute of Environmental Health Sciences, EMF RAPID (Electric and Magnetic Fields Research and Public Information Dissemination Program) website: http://www.niehs.nih.gov/emfrapid/home.htm
UC Berkeley Communication and Network Services Radio Frequency Safety. http://radio.cns.berkeley.edu/safety/rf-safety.shtml
United States Department of Labor, Occupational Safety and Health Administration. Non-Ionizing Radiation: Radiofrequency and Microwave Radiation. http://www.osha.gov/SLTC/radiofrequencyradiation/
World Health Organization, Electromagnetic Fields. http://www.who.int/peh-emf/en/

Management of RFID in Libraries

Boss, Richard *Library RFID technology.* in: Library Technology Reports, Nov/Dec 2003. 58 p.
McArthur, A *Integrating RFID into library systems - Myths and realities. Presentation at 69th IFLA General Conference and Council, 2003.* August, 2003 http://www.ifla.org/IV/ifla69/papers/130e-McArthur.pdf
Murray, P.E. *The Radio Frequency Revolution: Tips and Trends for Implementing RFID Systems in Libraries - University of Connecticut's Implementation.* January 28, 2004 http://www.pandc.org/peter/presentations/ala-2004-rfid/
San Francisco Public Library *RFID Implementation Proposaed Plan of Action* March, 31, 2004 http://www.sfpl.org/news/rfidplan.htm
San Francisco Public Library *RFID implementation: Proposed plan of action.* April 1, 2004 http://sfpl4.sfpl.org/librarylocations/libcomm/rfidplan040104.htm
Santa Clara City Library *Checkpoint RFID and the Santa Clara City Library* January, 2004 http://www.library.ci.santa- clara.ca.us/rfid/checkpoint.html

Santa Clara City Library. *Checkpoint RFID and the Santa Clara City Library.* January, 2004 http://www.library.ci.santa- clara.ca.us/rfid/checkpoint.html
Schneider, Karen *RFID and Libraries: Both Sides of the Chip* November 19, 2003 http://www.ala.org/ala/oif/ifissues/rfidbothsideschip.pdf
Smart, Laura *Making Sense of RFID* NetConnect, Oct. 15, 2004. pp. 4-14.

Privacy Concerns

AIM, Inc. *RFID connections - ROI of privacy invasion.* http://www.aimglobal.org/technologies/rfid/resources/articles/jan04/0401-roispy.htm
Anderson, Laura *The Library Defends its Principles: Privacy, Freedom, Access* in: Berkeley Daily Planet, February 25, 2005 http://www.berkeleydaily.org/article.cfm?issue=02-25-05&storyID=20819
Cavoukian, Ann *Guidelines for using RFID tags in Ontario public libraries.* Toronto, Ontario: Information and Privacy Commissioner http://www.ipc.on.ca/docs/rfid-lib.pdf
Cavoukian, Ann *Tag, you're it: Privacy implications of radio frequency identification (RFID) technology.* Toronto, Ontario: Information and Privacy Commissioner. February, 2004 http://www.ipc.on.ca/docs/rfid.pdf
Chachra, Vinod and Daniel McPherson *Personal privacy and use of RFID technology in libraries* VTLS. October 31, 2003. 7 p. http://www/vtls.com/documents/privacy.pdf
Consumers against Supermarket Privacy Invasion and Numbering (CASPIAN) *Position statement on the use of RFID on consumer products.Position statement on the use of RFID on consumer products.* http://www.privacyrights.org/ar/RFIDposition.htm
Good, Nathan et al. *Radio Frequency Id and Privacy with Information Goods* Paper given at the Workshop On Privacy In The Electronic Society. Washington, D.C., October 28, 2004. Washington, D.C. Association for Computing Machinery. http://delivery.acm.org/10.1145/1030000/1029193/p41-good.pdf?key1=1029193&key2=8203898211&coll=ACM&dl=ACM&CFID=57028760&CFTOKEN=16066961
(longer version)
http://www.law.berkeley.edu/clinics/samuelson/projects_papers/2004sp_rfid_WPES_draft.pdf
McIver, Rich *RFID Privacy Issues: How RFID Will Impact Consumer Privacy* in: RFID Gazette, March 22, 2005 http://www.rfidgazette.org/2005/03/rfid_privacy_is.html
Molnar, David and David Wagner *Privacy and Security in Library RFID: Issues, Practices, and Architectures* Paper presented at CCS'04, October 25-29, 2004, Washington D.C. Assocation of Computing Machinery, 2004. pp. 210-219
Molnar, David, and Wagner, D.A. *Privacy and security in library RFID: Issues, practices and architectures.* June 8, 2004 http://www.cs.berkeley.edu/~dmolnar/library.pdf
Privacy Rights Clearinghouse *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations* November, 20, 2003 http://www.privacyrights.org/ar/RFIDposition.htm
Samuelson Law, Technology, and Public Policy Clinic (the Clinic) at the University of California-Berkeley's Boalt Hall School of Law
RFID Vendor Assessment Tool

http://www.law.berkeley.edu/clinics/samuelson/projects_papers/2004sp_rfid_vendor_assessment_tool.pdf

Vendor Evaluation Framework
http://www.law.berkeley.edu/clinics/samuelson/projects_papers/2004sp_rfid_vender_evaluation_framework.pdf

Best Practices
http://www.law.berkeley.edu/clinics/samuelson/projects_papers/2004sp_rfid_best_practices.pdf

San Francisco Public Library. *Privacy Policy.* April 30, 2004
http://www.sfpl.org/librarylocations/libcomm/pdfs/privacypolicy.pdf

Schuyler, M. *RFID: Helpmate or conspiracy?* Computers in Libraries, 22 - 24. January, 2004

Tien, Lee *Privacy risks of radio frequency identification "tagging" of library books* Electronic Frontier Foundation, October, 2003
http://www.eff.org/Privacy/Surveillance/RFID/20031002_sfpl_comments.php

Tien, Lee *RFID and libraries: EEF talking points for the ALA IFC.* Summary of presentation to the ALA Intellectual Freedom Committee of the American Library Association ALA Mid-Winter Conference, San Diego, California. January 10, 2004 http://www.privacyrights.org/ar/RFID-ALA.htm

Warfield, Peter and Lee Tien *RFID Should be Canceled Immediately* in: Berkeley Daily Planet, March 4, 2005 http://www.berkeleydaily.org/text/article.cfm?issue=03-04-05&storyID=20871

RFID Resources

EPC Global Consortium http://www.epcglobalinc.org
EPC Global, Inc. http://www/epcglobalinc.org
RFID Gazette Los Angeles, Dotmarketer http://www.rfidgazette.org/libraries/index.html
RFID Gazette http://www.rfidgazette.org/
RFID Journal http://www.rfidjournal.com/
Campbell, Anita *RFID Weblog* http://www.rfid-weblog.com/

Return on Investment (ROI)

_____*New ROI Calculator for RFID* in: RFID Journal, May 5, 2003
http://www.rfidjournal.com/article/articleprint/407/-1/1

Curtin, John, Robert J. Kauffman, Frederick J. Riggins *Making the 'Most' out of RFID Technology: a Research Agenda for the Study of the Adoption, Use and Impacts of RFID* Minneapolis, Carlson School of Management, University of Minnesota, February 17, 2005

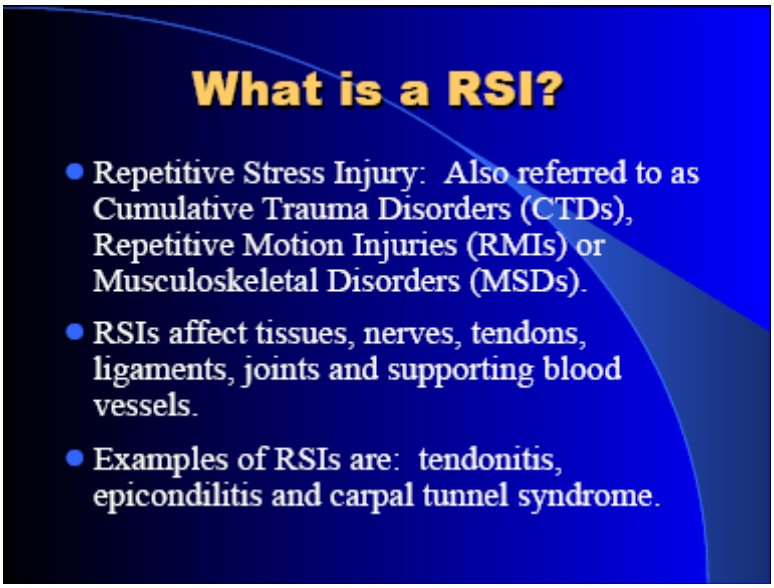
Veeramani, Raj *The Key to Finding RFID's ROI* in: RFID Journal, June 6, 2005
http://www.rfidjournal.com/article/articleprint/1635/-1/1

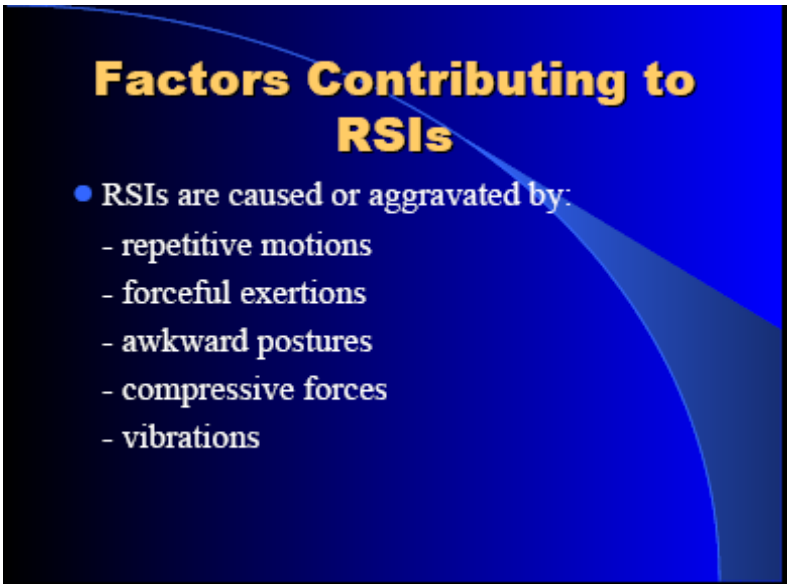
Appendix A: San Francisco Public Library - First Floor Remodel Progress Report. April 10, 2003

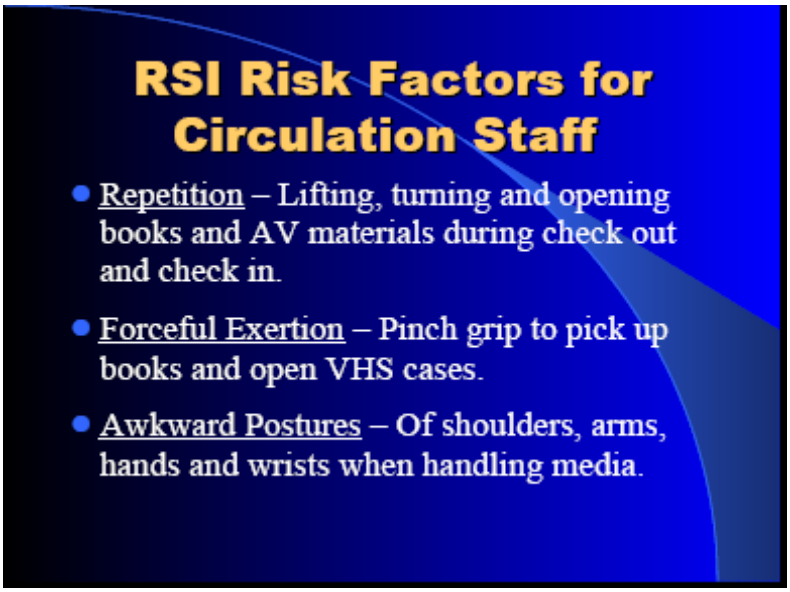
Appendix A is now located at the end of this report on page 70.

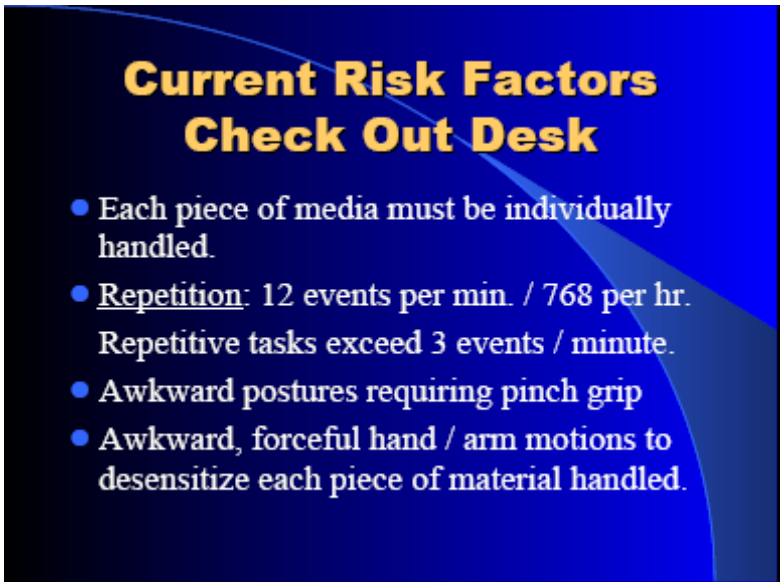
Appendix B: Repetitive Stress Injuries (RSIs), A Presentation to the Library Commission

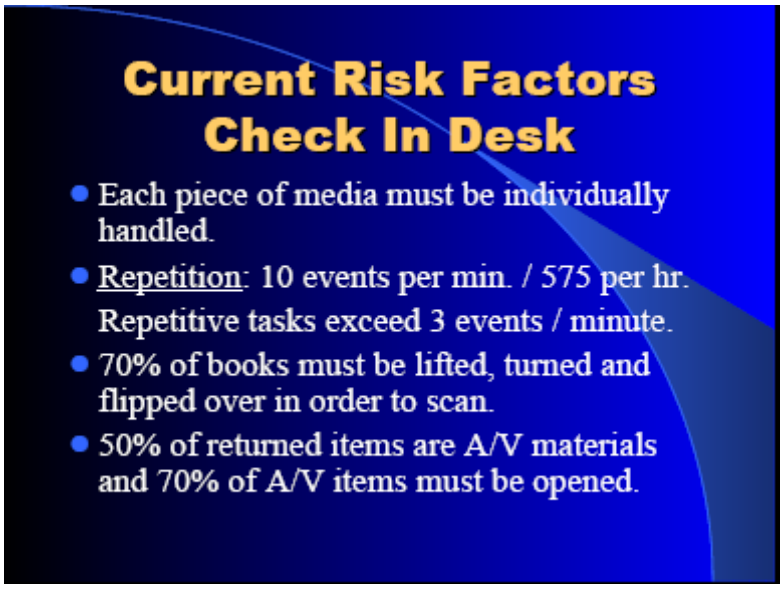
On April 1, 2004, Nancy Terranova, of the San Francisco Department of Public Health, gave a presentation to the Library Commission regarding Repetitive Stress Injuries in relation to circulation tasks. The slides of that presentation are below.

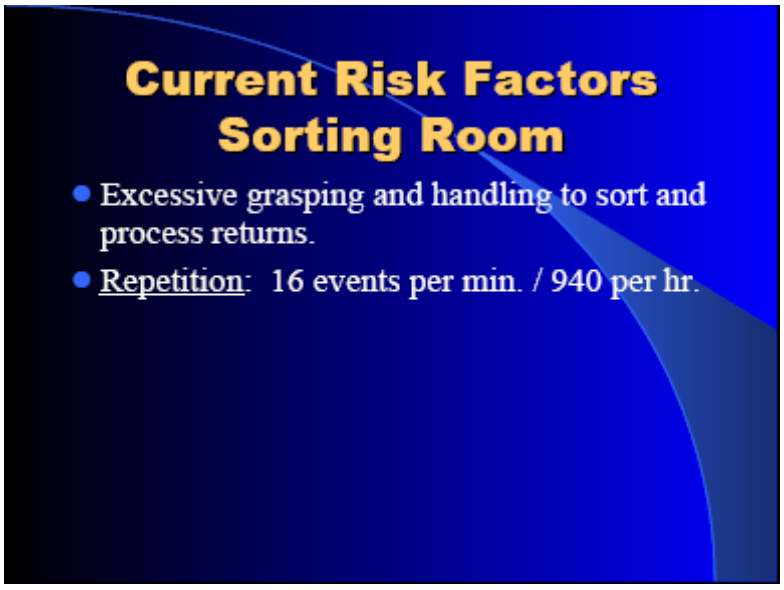




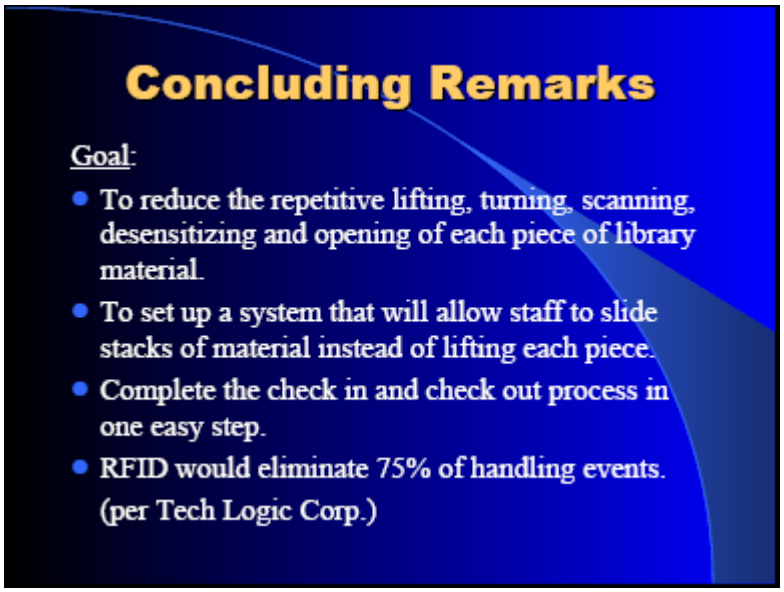

RSI Risk Factors for Circulation Staff
Repetition – Lifting, turning and opening books and AV materials during check out and check in.
Forceful Exertion – Pinch grip to pick up books and open VHS cases.
Awkward Postures – Of shoulders, arms, hands and wrists when handling media.


Current Risk Factors Check Out Desk
Each piece of media must be individually handled.
Repetition: 12 events per min. / 768 per hr.
Repetitive tasks exceed 3 events / minute.
Awkward postures requiring pinch grip
Awkward, forceful hand / arm motions to desensitize each piece of material handled.


Current Risk Factors
Check In Desk
Each piece of media must be individually handled.
Repetition: 10 events per min. / 575 per hr.
Repetitive tasks exceed 3 events / minute.
70% of books must be lifted, turned and flipped over in order to scan.
50% of returned items are A/V materials and 70% of A/V items must be opened.


Current Risk Factors
Sorting Room
Excessive grasping and handling to sort and process returns.
Repetition: 16 events per min. / 940 per hr.


Industrial Injury Rates
SFPL
From January 2001 through January 2004:
36 reported RSIs
260 loss work days
500 modified / restricted work days
$265,000 paid costs


Concluding Remarks
Goal:
To reduce the repetitive lifting, turning, scanning, desensitizing and opening of each piece of library material.
To set up a system that will allow staff to slide stacks of material instead of lifting each piece.
Complete the check in and check out process in one easy step.
RFID would eliminate 75% of handling events. (per Tech Logic Corp.)

Appendix C: Vendors Consulted

- Bibliotheca RFID Library Systems Inc. http://www.bibliotheca-rfid.com/
- Birchard Company http://www.birchard.biz/
- Checkpoint Systems, Inc. http://www.checkpointlibrary.com/
- ColorMarq Library Collection ID Systems http://www.colormarq.com/
- FKI Logistex http://www.fkilogistex.com/
- Integrated Technology Group http://www.integratedtek.com/
- Libramation Inc. http://www.libramation.com/
- Library Automation Technologies
- http://www.latcorp.com/latsite/index.html
- Tech Logic Corporation http://www.tech-logic.com/
- VTLS Inc. http://www.vtls.com/
- 3M Library Solutions
- http://cms.3m.com/cms/US/en/2-115/cerlRFW/view.jhtml

Appendix D: California Polytechnic State University RFID Survey, Fall 2004

From October 13, 2004 to November 1, 2004, Professor Jay Singh (Industrial Technology department), Navjit Brar (Assistant Dean at the Kennedy Library, and Carmen Fong (Industrial Technology student) from California Polytechnic State University, surveyed participating libraries, RFID listserv, and LITA-L listserv subscribers and collected information with regards to the implementation of RFID systems in libraries. Members and subscribers were given a link directing to an internet based survey. 29 completed the survey. The survey provided information with regards to the performance of such systems already in place and expectations from those being planned. Results from this survey are presented below.

Respondent Demographics

Out of the 29 survey participants, 26 are from public library, 2 from academic, and one of them is from a corporate library. Their collection size ranges from less than 1 million to more than 5 millions, with an average collection size of 1.34 millions from these libraries. The hours of operations per week for these libraries range from less than 50 hours to a maximum of 150 hours. The average hours of operations are 103.5 hours. Annual circulations of these library ranges are from 0-1 million to more than 3 millions volumes. 48% of the survey participants have an annual circulation of 0-1 million, 31% have 1-2 million volumes, and the rest of 10% have more than 3 millions volumes.

Majorities of the library participated in this survey are public libraries. Majority of the library have collection size of fewer than 2 millions copies, which consists of a total of 97% of all participants. 89% of all survey participants have less than or equal to 2 million users visit every year. 52% of the participating libraries have seating capacity for 0-200 people, 26% have 201-400, 11% have 401-600, 7% have 601-800, and remaining 4% have seating capacity for more than 1000 people.

Even though the majority of these participating libraries are relatively smaller libraries, but their interlibrary loan transactions are does not fall into their suppose trends (smaller libraries have less interlibrary loan transactions. 25% of the participating libraries have less then 500 copies for interlibrary loan transactions, another 25% have 500 to 1000 volumes, 11% have 1001 to 1500 copies, another 11% have 1501 to 2000 copies, while the remaining 29% have over 2000 copies in interlibrary loan transactions.

Q: Have you migrated to RFID?

Of the 29 survey respondents, only less than half of them have migrated to RFID. Those who have, consists of 38%, and the remaining 62% have not. The following table consists of responses from the 62% who have not migrated to RFID. Out of these 19 responses, 13 respondent (68%) currently are in the process of migrating to RFID, 4 respondents (21%) are considering, while 2 respondents (11%) have no current plans for RFID migration in their libraries.

#	Response
1	thinking about it; no date yet
2	One branch fully functional. Others coming in the next two years.
3	Process of evaluation
4	Winter 2004-2005
5	probably within two years
6	1 year
7	No current plan to.
8	FY2004-05
9	January - December 2005
10	probably in 2007
11	18-month project, beginning Nov. 2004
12	1-3 years
13	1-2 years
14	Jan-05
15	Early 2005
16	within next 4 years
17	We are investigating RFID - in fact we have a demo today from Checkpoint
18	We are currently tagging our collection. Expected to finish tagging and go live in Spring 2005.
19	NEVER!

Q: What was the conversion cost to RFID?

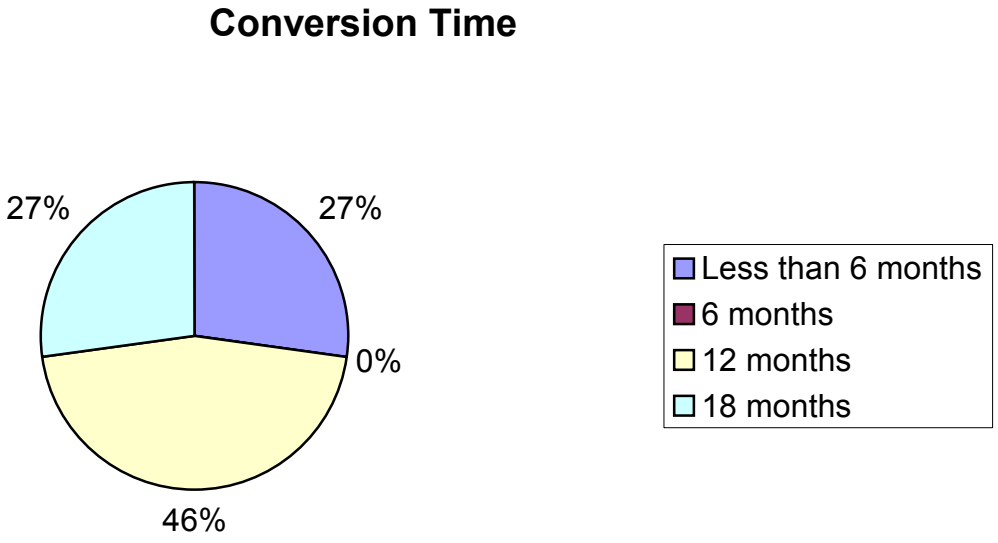
The conversion cost ranges from $113,000 to $1.2 million. Average conversion cost is $502,917(Results drawn from quantitative responses).

#	Conversion Cost
1	$ 1,200,000.00
2	$ 475,000.00
3	$ 300,000.00
4	$ 180,000.00
5	$ 1,200,000.00
6	$ 275,000.00
7	$ 750,000.00
8	$ 500,000.00
9	$ 142,000.00
10	$ 113,000.00
11	$ 250,000.00
12	$ 650,000.00

Maximum	$1,200,000.00
Minimum	$ 113,000.00
Average	$ 502,916.67

Q: How much was conversion time?

Conversion times for 11 libraries that have migrated to RFID vary from one library to another. 3 (27%) of those libraries took less than 6 months, 5(46%) libraries took 12 months, and the remaining 3(27%) took 18 months to switch to RFID. The average conversion time was 11.18 months.



Others who have not yet implemented RFID or those who are in the process of doing so provided time estimations or their current status.

#	Response
1	Have not yet started retro conversion.
2	Estimate 8 months
3	we expect to spend 12 months converting
4	N/A
5	6 to 9 months expected

The following responses are a comparison for workflow prior and post RFID from the 11 respondents who answered "Yes" on question, "Have you migrated to RFID?"

Respondent	Workflow prior to RFID	Workflow post RFID
1	Barcodes, light pens and multidirectional scanners, 2 self-check stations with limited capability, 8 stations assisted checkout. Hand check-in of all materials	RFID antennas used to check out and in. All stations are primarily self-checkout. All materials (other than very oversized) are returned and checked in by the automated system.
2	All transactions individually handled. No patron self checkout	Self Checkouts at three branches. One branch fully implimented with automatic bookdrop checkin. More time for staff to interact with patrons.
3	Check-in: Required a two-step process: scan the barcode to check-in on the automation system, then re-sensitize the magnetic security piece. Check-out: We used self-checkout at a 65-70% rate prior to RFID, however there was a high learning curve to operate the machines independantly. Materials Processing: Placement of barcode on outside cover of materials as determined by self-checkout positioning requirements. Often had to cover up UPC barcode to prevent interference and false scans. Item searching: Lists of items to be searched were manually printed to paper and staff or voluntees were assigned to search for materials. Required training and familiarity with Dewey and shelving rules and practices.	Check-in: RFID reduced this process by half; only one scan of the item is needed to check-in and re-activate the RFID tag. There is no longer any backlog of materials awaiting checkin, resulting in materials reaching the shelves faster and promoting a faster turn-around time. Check-out: Self-checkout stations were faster and easier to use, did not require alignment of item barcodes. Self-check usage jumped within a month to the current 90-95% rate. Materials processing: RFID tag placement on books is in standard location inside cover. Tag is hidden on media materials; for DVD, CD, CD-ROM, tag is on case and not material. Corresponding barcode appears inside book/case and positioning is not determined by self-check needs. Item searching: Lists of items are downloaded to portable inventory wand/handheld. Minimal training of staff and volunteers on wand required, no knowledge of shelvings practices required. Handheld unit emits audio alert and displays title, location and barcode of item to be pulled. More accurate searching.
4	No Response	Added patron self checkout and portable inventory devices for inventory
5	Not sure I understand the question. We used barcodes	Use selfcheck (100%) and Tech Logic sortation for returns and checkins.
6	log jams at circulation desk and checkins; increased workload with stagnant staffing levels	No lines at circulation during our busiest month in history, increased usage of self-checks

7	Long lines at checkout; each circulation transaction took 5 separate steps; did not have self-checkout available for public	Self-checkout machines used for 45% of total circulation; circulation transactions faster, fewer steps and less repetitive motion. Reallocation of some circulation staff to public service desks due to time savings using RFID.
8	BC scanning for circulation procedures. Some books had to be opened.	RFID tags scan if in proximity to antenna - sometimes a problem. No more opening of items - saves some time. CS and CD still need inspection for total number of items in the cases. Some CD and DVD will not accept RFID tag. Tags are 'dying' - unknown cause - age? damage? Check in is faster perhaps. We do 30,000 items /month at our branch. Security gates can give false alarms.
9	Multi-tasking -- Checking out desensitizing separate tasks, Checkin/resensitizing separate tasks.	Much improved --faster -- checkin/checkout sensitizing functions single action. Self check stations more efficient
10	Backlog of materials waiting to be checked in. Lines at desk for check out.	Faster check out and check in of materials. Less waiting. Also using patron self check.
11	what are you asking for here?	see #11

Q: How many staff you had?

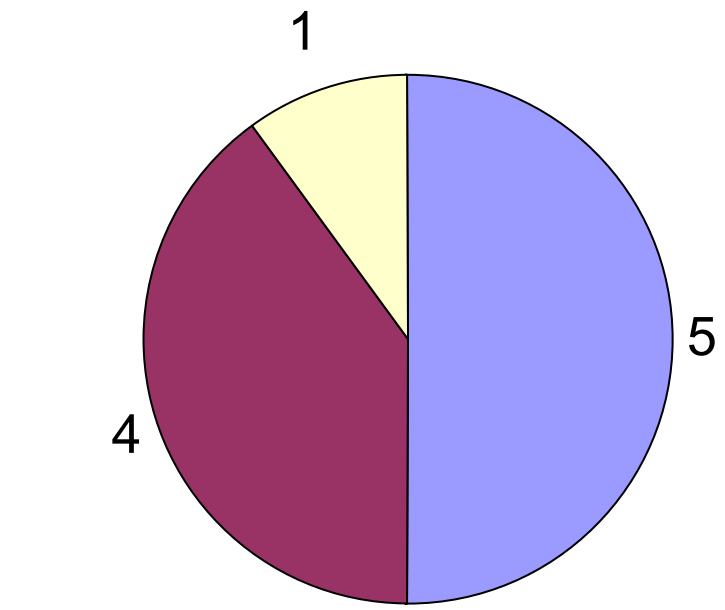
#	Prior to RFID	Post RFID	Comments
1	70	125	Moved to a larger building
2	>100	>100	
3	76	76	
4	50	56	New library
5	30	30	
6	543	543	
7	128	128	
8	117	no response	
9	same	same	
10	29.25	29.75	# of FTE reported here
11	130	no response	
12	58.6	72.24	doubled size of facility
13	68	N/A	
14	7	7	
15	35	35	
16	61	61	
17	33	33	
18	same	same	

There were no significant change in staff number before and after the conversion of RFID from participated libraries.

Q: Has the library usage increased since RFID implementation?

There were 10 responses for this question # 14. 50% of the participating library has shown more than 10% increase in usage since RFID implementation.

Percent Increase	Number of Respondents
0-10%	5
11-20%	4
21-30%	0
31-40%	0
41-50%	0
50%+	1



Q: How much staff time have you saved since the installation of RFID?

Few respondents have quantitative measurement of such value.

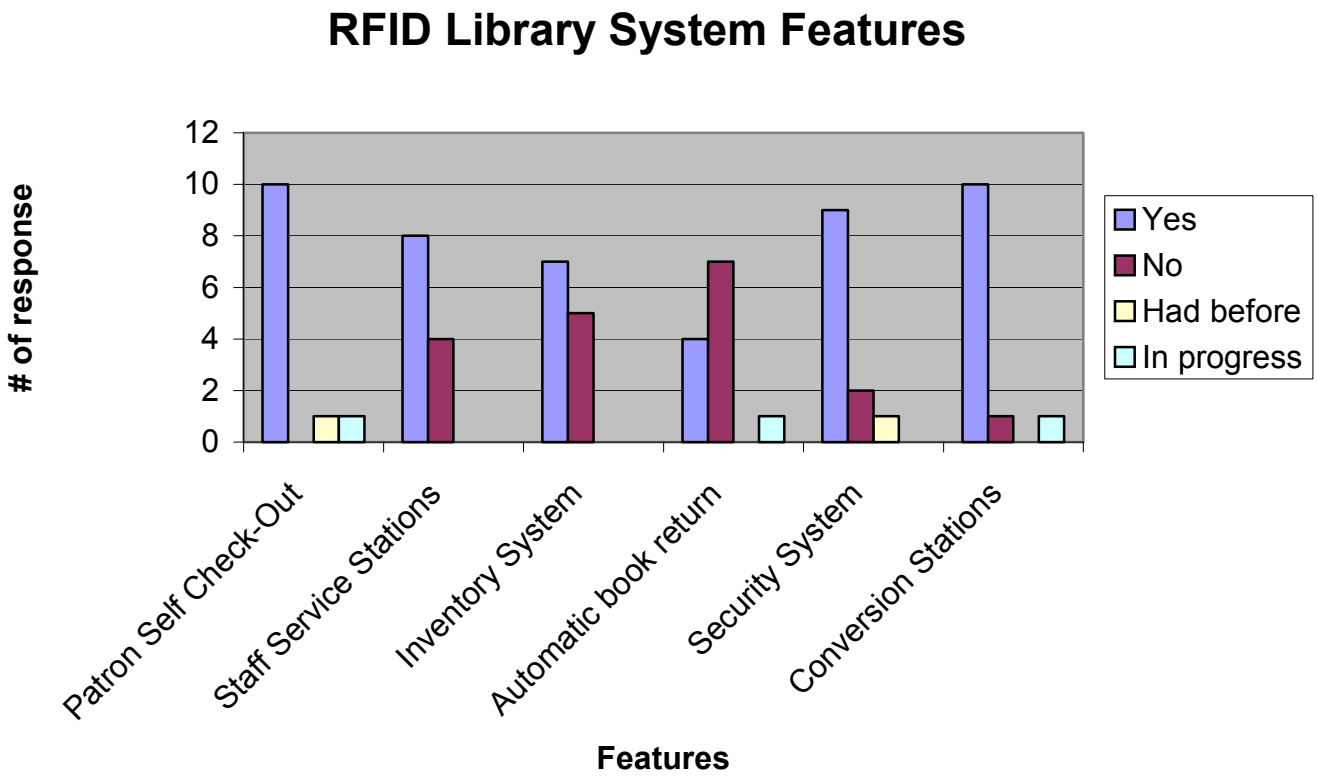
#	Response
1	Ha.
2	Can't yet calculate but with two new branches opening we will not be hiring more circ staff. We will just reassign them.
3	Check-in staff time has decreased by half. Check-out staff time has decreased by 25% -- staff time with direct contact now focuses on new account creation, paying fines, resolving larger issues vs. rote check-out.
4	Not calculated due to other circumstances.
5	Have not done studies. We've added no staff for checkin, but have added pages for shelfing.
6	Evidence of a great deal, but done no specific studies as yet.
7	About 60 hrs/wk circulation library assistants; deployed to other areas & service desks; staff savings allowed us to open a new larger facility with minimal increase in staff
8	N/A
9	Unknown - a great deal of time 'up front' of the project was troubleshooting - because we were a Beta test site.
10	20% Have not reduced staff, but transferred to other function. Using the DLA has saved a tremendous amount of time weeding/shelf reading.
11	Too soon to know.
12	still working on implementation

Q: Average check in and check out time before and after RFID installation?

Check-in time and check-out time both reported improvement—time reduction.

#	Average Check-in Time		Average Check-out Time	
	Spend Before	Spend After	Spend Before	Spend After
1	?	? But it is certainly faster	?	? But it is certainly faster
2	one hour/cart	30 minutes/cart	One minute	30 seconds
3	2 minutes		3 minute	
4	Done manually	Done by Tech Logic Sortation	One item at a time	mulitple items, but all selfcheck
5	1 mintues/item	15 seconds/item	30-45 seconds/item	5-10 seconds/item
6	<10 sec. Per item	N/A	<10 sec. Per item	N/A
7	unknown	unknown	unknown	unknown
8	? 2 step process--scan barcode/resensitize	? Single process--no scanning of barcode	? 2 step process--scan barcode/resensitize	? Single process--no scanning of barcode
9	minutes	seconds	minutes	seconds
10	2 min	1 min	4 min	3 min

Q: Have you implemented any of the following since RFID implementation?



Number of patron self-checkout stations ranges from 1 station to 9 stations. The average is 3.85 stations.

Response #	Patrons Self Check-Out Stations
1	**5**
2	**3**
3	**9**
4	**2**
5	**8**
6	**3**
7	**7**
8	**1**
9	**1**
10	**2**
11	**2**
12	**5**
13	**2**

Average	3.85
Maximum	9
Minimum	1

Q: Did you replace tattle tape with RFID barcodes?

	Number of Respondents
YES	8
NO	9

It is difficult to justify by simply analyzing a numeric amount of tattle tapes replaced, because this number does not reflect the relation to collection size of libraries.

#	Response
1	400,000
2	We did not use the 3M system. We have always been Checkpoint customers and use older RF system.
3	200,000
4	We are working on this
5	25,000
6	225,000
7	No, we had legacy Checkpoint system prior to RFID implementation
8	whole collection
9	Who collection

Q: What kind of training you received and recommend?

Survey respondents indicated that training was mostly done through vendor. Some respondents have felt their vendor provided adequate information and sufficient training while some didn't. Some respondents felt that system is user friendly, minimal training is required. Some felt that training needs to be further developed, but sharing information with the library community was helpful. Respondents recommended that training materials be documented for ease of referencing. Availability of training and "user's manual" information varies a great deal by vendors.

#	Response
1	Received little, got some placement sheets and a video to show volunteers.
2	On site by vendor.
3	Vendor staff trained core group of library staff who then trained additional groups of library staff. The trainers served as "experts" for questions during conversion. Core group of circulation and automation staff received training on the maintenance of the system's servers. Inventory wand training was conducted by vendor staff.
4	We are working on details with the vendor, estimate 4 training days for everything
5	Adequate.
6	We have 3 vendor training sessions planned. Not all library staff will attend the vendor training. We will use a train-the-trainer model for everyone else.
7	No formal training. They showed us how to do it and we did it, 250,000 times. It isn't brain surgery
8	Training is underdeveloped; worked with libraries with previous implementation for tips and tricks; worked closely and constantly with sales rep and vendor technicians
9	Training mainly in conversion of materials from vendor; other training was trial and error (we were the first library on the West Coast to implement RFID) Staff developed their own training materials.
10	N/A
11	Verbal at first - I highly rec. companies to have paperwork!! I spent a lot of time on the phone, e mails, downloading new versions of software, etc.
12	Our system is 3M, we received excellent training. Recommended.
13	Not much training really needed. System purchased is pretty self explanatory.
14	not enough and more - only brief overviews
15	Still in process. Training so far on programming tags.

Q: Would you recommend RFID to other libraries?

The following are responses from survey respondents who would recommend RFID to other libraries.

#	Response
1	Wave of the future! Important to patrons who are of the "I want it now, and to do it for myself" mindset.
2	There are so many things that can be done with RFID. I see many things in the future for it.
3	It has raised the efficiency of our operation. We have experienced steadily rising circulation and RFID has allowed us to meet that demand and still provide excellent service to our community. It has allowed staff time to work on projects that have been post-poned due to lack of staff time, as well as work on more interesting projects than rote check-in/check-out. We also have seen a change in exit-alarm responses, they are legitimate and not false alarms and we have a record of all items that left the building without checkout. These types of losses can now be noted in the catalog resulting in a more accurate representation of our holdings.
4	Yes
5	If a library can implement automated Check-in and sorting, as well as Self Check-out, the system saves staff time and repetitive stress handling.
6	If they can afford it, because I think it's faster and easier to use than most electromagnetic systems on the market.
7	I think it is very helpful if you have the sortation system. I'm not sure it is cost effective if you don't have sortation.
8	It's worth the conversion hassle to dramatically improve workflows in an environment where it's far easier to get technology dollars than staffing dollars.
9	Yes
10	We have realized benefits from RFID implementation. Ease of use, savings of time in transacation, and ability to interface with current and future technology such as materials return/sorting systems.
11	Even though we have yet to implement this technology, it seems to be far superior to the old systems (Tattle Tape) in so many ways. I am hopeful that it will serve us well for many years to come.
12	Technology is improving all the time. Tags are better than when we started 4 years ago. Save manipulation of materials (opening)- even tho the BC is on the outside of materials - it doesn't matter if you lay them face down or face up on the antenna. Also at self check out, 4 items may be checked out at once - tho the instructions/screens are rather long!
13	Greatly simplifies circulation activities.
14	Faster, faster, faster! Reduces lines at desk which reduces staff stress. Simple self check procedures empower patrons.
15	cuts theft, decreases range of motion injuries
16	We can see already that when implemented this will simplify the check out process for staff, save staff time which can be redeployed to other tasks and reduce worker's comp repetitive stress injuries.
17	I wouldn't recommend rfid tags. They are an INVASION OF PRIVACY and have NO BUSINESS in libraries or anywhere else!

The following are responses from survey respondents who would not recommend RFID to other libraries.

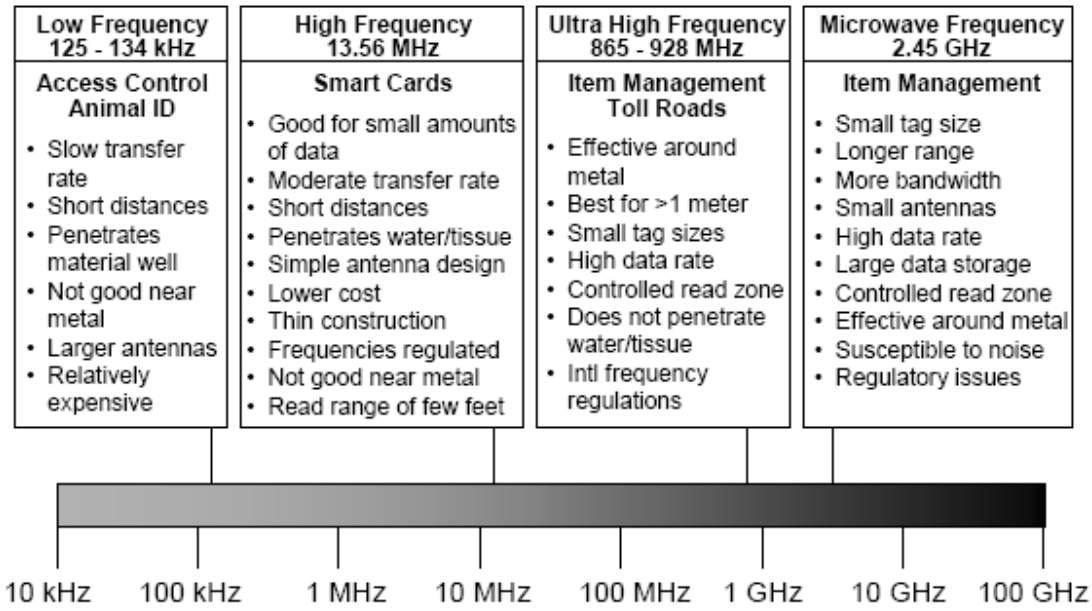
#	Response
1	The conversion is difficult to justify during a time of reduced budgets, the Return on Investment when calculating minimal time saved on common jobs doesn't offer any immediate or even short range return on the effort. In addition, tattle tape will still need to be used for security, as RFID has no real security feature according to manufacturers I've talked with (including 3M). It's just too cost prohibitive for smaller University Libraries.
2	Because they are an INVASION OF PRIVACY and have NO BUSINESS in libraries or anywhere else!

The two respondents who object to RFID use in the library systems fear the financial impact RFID will bring because of its considerable amount of initial investment and thus may not be suitable for smaller libraries. Others fear the privacy issues that RFID will bring.

New technologies are often perceived as job eliminators. RFID, in this case, did not have such effect. RFID helped to reduce worker injuries such as repetitive stress syndrome caused by opening and closing books, falling injuries caused by reaching top shelves during inventory count process and other related injuries caused by normal library operations.

We should conduct another survey to ask more specific questions, and to limit the answer parameter—to give more specific instructions about the kind of answers that we are looking for, whether it's quantitative, comments etc.

Appendix E: The Most Popular RFID Read Range Frequencies[45]



[45] John Curtin, Robert J. Kauffman and Frederick J. Riggins. Making the 'Most' Out of RFID Technology: A Research Agenda for the Study of the Adoption, Use and Impacts of RFID. February 17, 2005. P. 8. http://misrc.umn.edu/workshops/2005/spring/ckr_itm2005_rfid_021705.pdf

Appendix F: American Library Association's Intellectual Freedom Committee's (IFC) DRAFT Guidelines on RFID Implementation

Radio Frequency Identification (RFID) is a method to collect, use, store, and broadcast data. Components include tags, readers, computer hardware (such as servers and security gates) and RFID-specific software.

When used in libraries, this technology enables efficient and ergonomic inventory and circulation operations. While RFID can enhance individual privacy through self-checkout of library materials, the technology also raises serious privacy and intellectual freedom concerns because RFID tags can be read by unauthorized individuals using an RFID reader.

At its 2005 Midwinter Meeting in Boston, the American Library Association adopted the Book Industry Study Group's (BISG) "RFID Privacy Principles,"[1] and directed that the ALA develop guidelines for the implementation of RFID technologies in libraries. ("Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles,"[2] adopted by the ALA Council on January 19, 2005, Boston, Massachusetts.)

Basic Privacy Principles

Protecting user privacy and confidentiality has long been an integral part of the mission of libraries. The right to free inquiry as assured by the First Amendment depends upon the right and the ability to read and access information anonymously, free from scrutiny. Librarians have an ethical obligation to preserve the library user's right to privacy in the library, and to prevent any unauthorized use of the library user's personal information.

Policy Issues for Libraries Implementing RFID Technologies

- Libraries implementing RFID technologies should adopt and update appropriate policies and procedures in order to protect library users' privacy, in compliance with Article III of the ALA Code of Ethics[3] and *Privacy: An Interpretation of the Library Bill of Rights*[4]. Such policies should be transparent about the library's use of RFID technologies. The *Guidelines for Creating a Privacy Policy*[5] can assist libraries in drafting appropriate policies.
- Notice and information about the library's use of RFID technologies should be posted prominently and made widely available to the public, both within the library and through the library's print and online communications.
- Libraries should educate and inform library users concerning RFID technology and its current and future use in the library and in society as a whole in order to give users a larger voice in the public debate over RFID technology.

- Libraries should disclose any changes in their privacy policies or in their terms of use for patron data that result from the adoption of an RFID system.
- In relation to their use of RFID technologies, libraries should recognize their institutional obligations with respect to notice, access, use, disclosure, retention, enforcement, security, and disposal of records.
- Libraries should not use RFID systems to track individual library users. Libraries should remove any personally identifiable information from statistical data collected by RFID systems.
- Libraries should train staff to protect user privacy in conjunction with the implementation and use of RFID technologies.

Technology Issues for Libraries Implementing RFID Technologies

- Libraries should affirm and reinforce their obligation to secure their bibliographic and patron database from unauthorized entry.
- Libraries should protect their RFID databases in the same way that they ensure the security of the circulation and other functions of integrated library systems (ILS).
- Due to the potential for eavesdropping, libraries should use hardwire connections and not wireless connections for all communications between RFID systems and the ILS involving personally identifiable information.
- Libraries should encrypt information stored on RFID tags.
- Libraries should limit the information stored on the tag to the item's barcode.
- Libraries should refrain from storing personally identifiable information (PII) on RFID tags or RFID-enabled patron cards.
- Libraries utilizing "smart cards" should use an "opt-in" system that allows library user to choose between "smart cards" and barcode-enabled cards in order to accommodate users who do not wish to utilize or carry an RFID-enabled device. (Technology to accommodate a hybrid card system is available from vendors without significant additional expense.)
- Libraries should clearly identify all of their RFID readers so that users know they are in use.

- ♣ Libraries should not grant individuals the ability to search the library's catalog by barcode number, in order to avoid linking a specific information item to a specific user. In addition, staff should be trained to not release information about the barcode in response to blind or casual inquiries.

Vendor Issues for RFID Technologies

- ♣ Librarians should be aware that independent researchers have concluded that current RFID technology cannot preserve user privacy in the library.[6] RFID is a technology with evolving standards and while encryption technology to enhance user security is under development, it is not widely available.
- ♣ The agreement between the library and the vendor should stipulate how the system will secure all information and guarantee library control of all data. Assurances of library users' privacy by vendors should be closely investigated. Libraries should evaluate the vendor's agreement in relationship with all library privacy policies and local, state, and Federal laws.
- ♣ Libraries should work to influence the development of RFID technologies by issuing Requests for Proposals to vendors that require the use of security technologies that preserve privacy and discourage monitoring.
- ♣ Librarians should educate themselves about RFID technologies and their associated industries, and continue to monitor news and reports concerning changes in the technologies and any new information concerning the privacy and health of library users. Libraries should be prepared to adjust their policies and procedures in light of new information.

[1] http://www.bisg.org/docs/BISG_Policy_002.pdf

[2] http://www.ala.org/ala/oif/statementspols/ifresolutions/rfidresolution.htm

[3] http://www.ala.org/oif/policies/codeofethics

[4] http://www.ala.org/oif/policies/interpretations/privacy

[5] http://www.ala.org/oif/iftoolkits/privacy/guidelines

[6] David Molnar and David Wagner, Privacy and Security in Library RFID: Issues, Practices, and Architectures, CCS'04, October 25-29, 2004 Washington, D.C.

SFPL Main- 1st Floor Remodel Project Progress Report April 10, 2003

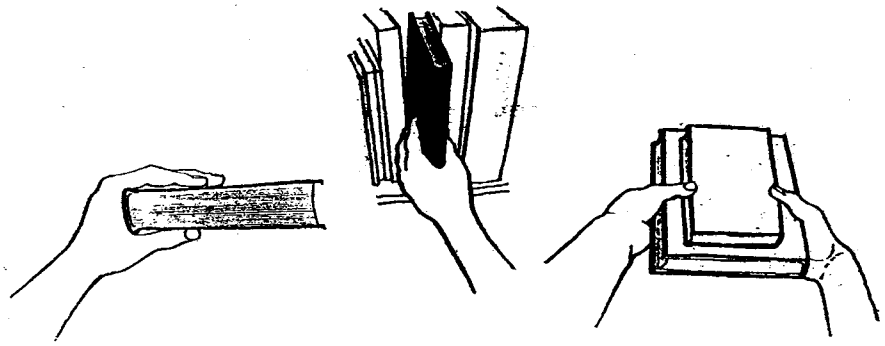
Project Objective
Improve the ergonomic and workflow conditions for the 1st floor Borrower Services, ILL, AV and Sorting Room staff and integrate the material flow among these groups.

Meeting Objectives
- Understand ergonomic and workflow problems and get consensus on resolving them
- Review preliminary designs and set direction for proceeding with most promising concepts
- Develop action plan and delegate responsibilities for the following:
  - procuring materials and testing concepts
  - group meetings to validate, refine and approve concepts

Primary emphasis of this meeting is to advance the PROBLEM SOLVING process

General Problem Statement
The majority of the staff performs short-cycle hand activities over the day to process and circulate library materials. These activities involve large daily doses of repetitive hand manipulation of materials that require pinch gripping, the use of force and / or awkward hand / wrist and arm postures. These are all known risk factors that contribute to the developments of Work-related Musculoskelatal Disorders (WMSDs) and must be minimized to the extent feasible.

Problem Solving Antedote: THE STAFF HAVE NO THUMBS



Explanation:
If the staff had no thumbs, no opposing grip capability, they would be unable to grasp items, pinch grip items, twist or flip items or open items like AV jackets- the things we <u>don't</u> want them doing anyway.
What would we have to do to accommodate a library staff that had no thumbs and still get work done?
- Design all counter, processing and sorting stations to allow the staff to <u>slide</u> rather than grasp and lift materials
- Improve the <u>reach</u> metrics of all functions to allow materials to be <u>raked or swept</u> with the hands to move them toward and away from the body
- Provide them with 4-fingered gloves

"NO THUMBS" can be used as a measure to evaluate the merit of proposed design concepts.

1. Return Desk- Ergonomic / Workflow Findings

Problems:

1. EXCESSIVE GRASPING AND HANDLING TO PROCESS RETURNS
   - 10 events per minute / 575 per hour
   - involve risk factors pinch grip, force and awkward postures
   - Staff Survey rank order importance # 4, 5 and 6

Recommendations:

a. Improve countertop scanning (omni-directional) and security equipment to slide material
b. Raise keyboards and LCD monitors off counters to slide material
c. Locate secondary equipment below counter to slide material, i.e., printer, resensitizer
d. Improve reach metrics of counter design to rake / slide material and maximize material flow and staging of media
e. Offload "simple" returns to Express Drop to reduce volume of materials and pace of work (60% potential)
f. Train staff on optimal media handling techniques
f. Barcode to front cover- ongoing
g. RFID would eliminate 75% of handling events (per Techlogic Corp)

2. USE OF FORCE TO OPEN AV MATERIAL
   - AV 50% of total return items processed / 70% were opened
   - Staff rarely used video opener jigs
   - Staff complained many CDs are broken making it difficult to open
   - Staff report it interrupts their rhythm and patron interaction
   - Staff Survey rank order importance # 1

Recommendations:

a. Do content verification for every 3rd item at each process point to share the load
b. Offload patrons to Express Drop to reduce volume and pace
c. Clear video jackets / windows (ongoing)
d. Solution for CDs???

3. AWKWARD POSTURES / INEFFICIENT FLOW AT RETURN SHELVES and SHUTE
   - Travel distance / congestion / carts
   - Awkward bending and reaching to deposit or retrieve
   - Staff Survey rank order importance # 3, 6, 7 and 8

Recommendations:

a. Rear wall with pass-through deposit of returns at optimum reach and distance metric
b. Retractable shelves for Reserves, 1st Stop and exception materials
c. No carts or bins permitted and no patron eye sores
d. Shared equipment bays at each end for cash registers and security equipment

4. RETURN COUNTER TOO DEEP FOR REPETITIVE REACHING
   - 28 inch depth to counter edge is too deep for 75% of females and 10% of males
   - Depth promotes grasping / pinch gripping of materials vs. raking and sliding

- Common observation and complaint by staff at interviews
- Staff Survey did not include (my oversight) but received 1 write-in vote

Recommendations:

a. Create counter positions with recessed body pocket cutaway (24" to front edge) to optimize reach and enable materials to be raked in rather than grasped
b. Maximize material flow and staging toward the inside left of each counter position
c. Mock-up and have staff use-test several designs

5. FOOTREST AT RETURN COUNTER
   - Staff Survey rank order of importance # 10

Recommendation

a. Design portable footrests w. different height each side to accommodate different staff sizes

6. RETURN COUNTER TOO HARD / TOO COLD
   - Surface temperature of stone is generally 25 degrees cooler (interior) than wood / plastic
   - Hard / cold counter was common complaint of staff at interviews
   - Stone surface is not smooth and resists sliding materials
   - Staff Survey rank order of importance # 12 but 7 of 17 ranked it in top 10

Recommendation:

a. Surface finish should be Corian or equal material with polished finish

7. RETURN COUNTER TOO HIGH / TOO LOW
   - Awkward postures not presented by staff but common complaint among staff
   - Staff Survey rank order of importance # 14 (last) with only 1 in top 10

Recommendation:

a. Counter set at 39 inch or alternate counter height at 39" and 42"

8. RESERVES ARE INNEFFICIENT AND INCONVENIENCE PATRONS
   - Staff Survey write-in vote by 6 of 17 surveyed- very significant!

Discussion item for team

2. Checkout Desk- Ergonomic / Workflow Findings

Problems:

1. AWKWARD AND EXCESSIVE HANDLING TO PROCESS CHECKOUT ITEMS
   - 12 events per minute / 768 per hour
   - involve risk factors pinch grip, force and awkward postures
   - Desensitizing non-magnetic media involves raised shoulder and shoulder extension
   - Staff Survey rank order importance # 3, 3 (tied) and 4

Recommendations:

a. Improve countertop scanning (omni-directional)
b. Design a block on counter to place non-magnetic desensitizer on it's side to slide materials across face / locate magnetic security on inside to avoid damaging videos
c. LCD monitors off counters to slide
d. Locate printer below counter to minimize raised arm and reaching
e. Improve reach metrics of counter design to rake and slide material and maximize material flow and staging toward the outside right / left of each counter position
f. Offload patrons to Self Check to reduce volume of materials and pace of work
g. Ensure counter positions have opening onto public space to assist patrons
f. Train staff on optimal handling techniques
h. Barcode to front cover- ongoing
i. RFID would eliminate 75% of handling events (per Techlogic Corp)

2. USE OF FORCE TO OPEN AV MATERIAL
   - AV 50% of total Checkout items processed / 70% were opened
   - Staff rarely used video opener jigs
   - Staff Survey rank order importance # 1

Recommendations:

e. Random content verification (every 3rd item) at each process point to share the load
f. Offload patrons to Self Check to reduce volume and pace
g. Clear video jackets / windows (ongoing)
h. Solution for CDs???

3. AWKWARD TWISTING AND BENDING TO CHECKOUT FROM SEATED POSITION
   - Extended reach required for printer and desensitizing due to equipment arrangement and "L" counter design
   - Knee clearance to patron position obstructed requiring twisted torso
   - Sitting compromises reach capability and stressful on spine
   - Some feet don't contact floor or foot ring from chair or stool
   - Staff Survey rank order of importance for bending forward bend, twist and reach were # 2 and 5. No foot contact was # 8.

Recommendations;

a. Checkout counters to be standing height at 39 inches
b. Optimize tool placement to facilitate reach from standing position
c. Raise tools above, place tools below or embed tools in counter to allow sweeping and sliding

4. LOCATION OF CHECKOUT OBSCURES LINE OF SIGHT AND CONFOUNDS QUEUE
   - Checkout location amidst columns and off patron path of travel obscures staff view and confounds queue
   - Staff Survey included 2 write-in votes on

Recommendations:
   - Checkout Desk counters in central queue area to make it obvious / macroscopic
   - Signage and lighting also issues to address at counters

5. CHECOUT COUNTER TOO HARD / TOO COLD
   - Hard / cold was common complaint of staff during interviews
   - Stone surface is not smooth and resists sliding materials
   - Staff Survey rank order of importance # 10 (last) but 7 of 15 ranked it in top 10

Recommendation:

b. Surface finish should be Corian or equal material with polished finish

3. Sorting Room- Ergonomic / Workflow Findings

Problems:

1. EXCESSIVE GRASPING AND HANDLING TO SORT / PROCESS RETURNS
   - 16 events per minute / 940 per hour
   - Involve risk factors repetitive pinch grip (minimal force or awkward postures)
   - Worst pinch grip condition observed at paperbacks densely packed on truck
   - Scan and resensitize branch returns is very repetitive and inefficient
   - Staff Survey rank order importance # 1, 2, 4 and 5

Recommendations:

a. Design a rough sorting system that allows the staff to slide materials
b. Develop a cart / transport system that allows materials to be swept from the book platform to a work surface- open gate or hatch
c. Design a fine sorting system that permits sort tables to be docked to rough sort carousel and / or carts and shelving to transfer materials easily
d. Have Return Desk presort high volume / readily identifiable materials, i.e., Children's, Foreign Language, to reduce handling by 25%
e. Investigate self-leveling trucks and possibility of sorting directly to truck versus table-to-shelf / shelf-to-rack / rack-to-truck which would reduce handling 50% of handling events

2. COMPLEXITY OF ROUGH SORT
   - Sort includes over 30 categories / many fragmented numeric sequences
   - Materials are double / triple handled to finalize block sort to shelves
   - Building trucks requires moving between shelf sections to gather materials per floor
   - Loaded trucks in numerical sequence are a mix of book type / genre and must be unloaded and resorted again on floors
   - Mixed loads partially due to stability of contents on moving trucks and 3rd floor backlog
   - Staff Survey rank order importance #3

Recommendations:

a. Design sorting system based on a "destination sort" concept by Floors / by Type
b. Label sorting bays with destination / numeric sequences to simplify sort and reduce double handling
c. Utilize magnetic shelf dividers an trucks to stabilize contents during transport

3. BENDING TO BOTTOM SHELF ON TRUCKS / IN SPRING-LOAD BINS
   - Bend and twist trunk significantly to retrieve material from spring-load bins that bottom out with 40 books
   - Bend and twist trunk to load and unload bottom shelves on trucks
   - Staff Survey rank order importance of bend to trucks and bins #6 and #6 tied

Recommendations:

a. Procure self-leveling bin with weight-calibrated springs for large volume staging / transporting
b. Integrate push-button hydraulic scissors lift for fixed, high volume material staging
c. Investigate self leveling truck system that raises and lowers as you load and unload materials
d. Staff should sit when loading trucks and stand when unloading trucks to alternate postures

4. PUSHING / PULLING LOADED BOOK TRUCKS (GRAY)
   - Forces to initiate movement are in excess of 40 pounds / on carpet > 60 pounds
   - Trucks are loaded to capacity to stabilize contents and / or to maximize truck availability due to 3rd floor backlog
   - Staff Survey rank order importance of push / pull trucks # 7

Recommendations:

a. Limit truck loading to top 2 shelves (when 3rd floor backlog is relieved)
b. Avoid using carpet in sort room
c. Investigate self leveling trucks (see Recommendation 3)

5. LIFTING BRANCH RETURNS BINS (GRAY BINS)
   - Lift an average of 25 bins at 50 pounds over 2 hour period from below knee height
   - Staff Survey rank order importance of push / pull trucks # 8

Recommendations:

a. Procure self-leveling bin cart to raise bins between knuckle and chest height
b. Or, procure simple dolly with raised platform to nest bins 3 high

Special Note: Branch Sorting / Distribution currently handle the same bins at much greater frequency than Main Sorting Room and could benefit from the self-leveling bin cart.